THE SMITH NORMAL FORM DISTRIBUTION OF A RANDOM INTEGER MATRIX

YINGHUI WANG AND RICHARD P. STANLEY

Abstract

We show that the density μ of the Smith normal form (SNF) of a random integer matrix exists and equals a product of densities μ_{p^s} of SNF over $\mathbb{Z}/p^s\mathbb{Z}$ with p a prime and s some positive integer. Our approach is to connect the SNF of a matrix with the greatest common divisors (gcds) of certain polynomials of matrix entries, and develop the theory of multi-gcd distribution of polynomial values at a random integer vector. We also derive a formula for μ_{p^s} and compute the density μ for several interesting types of sets. Finally, we determine the maximum and minimum of μ_{p^s} and establish its monotonicity properties and limiting behaviors.

1. Introduction

Let M be a nonzero $n \times m$ matrix over a commutative ring R (with identity), and r be the rank of M. If there exist invertible $n \times n$ and $m \times m$ matrices P and Q such that the product PMQ is a diagonal matrix with diagonal entries $d_1, d_2, \ldots, d_r, 0, 0, \ldots, 0$ satisfying that $d_i \mid d_{i+1}$ for all $1 \le i \le r-1$, then PMQ is the *Smith normal form (SNF)* of M. In general, the SNF does not exist. It does exist when R is a *principal ideal ring*, i.e., a ring (not necessarily an integral domain) for which every ideal is principal. This class of rings includes the integers $\mathbb{Z}$ and their quotients $\mathbb{Z}/q\mathbb{Z}$, which are the rings of interest to us here. In fact, for the rings $\mathbb{Z}/q\mathbb{Z}$ we will be particularly concerned with the case $q = p^s$, a prime power. For principal ideal rings, the diagonal entries are uniquely determined (up to multiplication by a unit) by $g_{i-1}d_i = g_i$ $(1 \le i \le r)$, where $g_0 = 1$ and g_i is the greatest common divisor (gcd) of all $i \times i$ minors of M. We have the following correspondence between the SNF and the cokernel of M: $\operatorname{coker} M \simeq R/d_1R \oplus R/d_2R \oplus \cdots \oplus R/d_rR \oplus R^{n-r}$.

There has been a huge amount of research on eigenvalues of random matrices over a field (see, e.g., [1], [2], [10], [12]). Less attention has been paid to the SNF of a random matrix over a principal ideal ring (or more general rings for which SNF always exists). Some basic results in this area are known, but they appear in papers not focused on SNF per se. We develop the theory in a systematic way, collecting previous work in this area, sometimes with simplified proofs, and providing some new results.

We shall define the *density* μ of SNF of a random $n \times m$ integer matrix as the limit (if exists) as $k \to \infty$ of $\mu^{(k)}$, the density of SNF of a random $n \times m$ matrix with entries independent and uniformly distributed over $\{-k, -k+1, \ldots, k\}$ (see Definition 3.1 below for a precise definition).

As a motivating example, the probability that $d_1 = 1$ for a random $n \times m$ integer matrix is the probability that the nm matrix entries are relatively prime, or equivalently, that nm random integers are relatively prime, and thus equals $1/\zeta(nm)$, where $\zeta(\cdot)$ is the Riemann zeta function.

If we regard the minors of an $n \times m$ matrix as polynomials of the nm matrix entries with integer coefficients, then the SNF of a matrix is uniquely determined by the gcds of the values of these polynomials (recall the definition of SNF from the beginning). This inspires us to study the theory of multi-gcd distribution of polynomial values.

Date: June 11, 2015.

Acknowledgements: The authors are grateful to Professor Bjorn Poonen for advice on the literature on the subject of this paper. The second author was partially supported by NSF grant DMS-1068625.

Given a collection of relatively prime polynomials in $\mathbb{Z}[x_1, x_2, \ldots, x_d]$, let $g(x)$ be the gcd of the values of these polynomials at $x = (x_1, x_2, \ldots, x_d)$. We shall define the *density* λ of $g(x)$ of a random d-dimensional integer vector x as the limit (if exists) as $k \to \infty$ of $\lambda^{(k)}$, the density of $g(x)$ with x uniformly distributed over $\{-k, -k+1, \ldots, k\}^d$ (see Definition 2.1 for a precise definition).

In the spirit of previous work in number theory such as [6], [14], [15] and the Cohen-Lenstra heuristics ([4], [5]), one might conjecture that λ exists and equals the product of density λ_p of $g(x)$ over $(\mathbb{Z}/p\mathbb{Z})^d$ over all primes p. In fact, we will prove this conjecture with the more general density λ_{p^s} of $g(x)$ over $\mathbb{Z}/p^s\mathbb{Z}$ for sets of form (2.5) (see Theorem 2.8), with the aid of a result in number theory [15, Lemma 21]. Note that the special case that $s = 0$ or 1 follows from [6, Theorem 2.3] directly. In particular, this result applies to the probability that $g(x) = 1$, in other words, that the polynomial values are relatively prime. Furthermore, all these results hold for the multi-gcd distribution of polynomial values, namely, when $g(x)$ is a vector whose components are the gcds of the values of given collections of polynomials at x.

Then we apply this theory to the SNF distribution of a random integer matrix to show that the density μ (of SNF of a random $n \times m$ integer matrix) equals a product of some densities μ_{p^s} of SNF over $\mathbb{Z}/p^s\mathbb{Z}$ for sets of form (3.4) (Theorem 3.8). We also derive a formula for μ_{p^s} (Theorem 3.2), which allows us to compute μ_{p^s} and hence μ explicitly (Theorem 4.3). Some special cases of this formula coincide with [16, Exercise 1.192(b)] and [9, pp. 233, 236]. Another paper related to our work is [17].

On the strength of these results, we determine the value of μ for some interesting types of sets, specifically, matrices with first few diagonal entries given, matrices with diagonal entries all equal to 1, and square matrices with at most $\ell\,(= 1, 2, \ldots, n)$ diagonal entries not equal to 1, i.e., whose corresponding cokernel has at most ℓ generators; further, for the last set we establish the asymptotics of μ as $\ell \to \infty$. In the case of $\ell = 1$ (which is equivalent to the matrix having a cyclic cokernel), our results echo those of Ekedahl [6, Section 3] via a different approach. We also show that the probability that a random integer matrix is full rank is 1, and that μ of a finite set is 0.

Additionally, we find the maximum and minimum of $\mu_{p^s}(D)$ over all diagonal matrices D; whereas regarding it as a function of p, s, m, n and D, we find its monotonicity properties and limiting behaviors.

The remainder of this paper is organized as follows. Section 2 develops the theory of multi-gcd distribution of polynomial values. Section 3 applies this theory to the SNF distribution and derives a formula for μ_{p^s}. Section 4 computes the density μ for several types of sets. Finally, Section 5 determines the maximum and minimum of μ_{p^s} and discusses its monotonicity properties and limiting behaviors.

We shall assume that throughout this paper, p represents a prime, p_j is the j-th smallest prime, and $\prod_p$ means a product over all primes p.

2. Multi-gcd Distribution of Polynomial Values

Suppose that d and h are positive integers and $F_1, F_2, \ldots, F_h \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ are nonzero polynomials. Let

$$g(x) := \gcd(F_1(x), F_2(x), \cdots, F_h(x)), \quad x \in \mathbb{Z}^d$$

be the gcd of the values $F_1(x), F_2(x), \ldots, F_h(x)$, and $g(x) = 0$ if $F_j(x) = 0$ for all $1 \le j \le h$.

We shall define the *density of $g(x)$ of a random d-dimensional integer vector x* as the limit (if exists) of the density of $g(x)$ with x uniformly distributed over $\{-k, -k+1, \ldots, k\}^d := \mathbb{Z}^d_{(k)}$ as $k \to \infty$, precisely as follows.

Definition 2.1. (i) For $\mathcal{Z} \subseteq \mathbb{Z}$, we denote by $\lambda^{(k)}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z}$ with x uniformly distributed over $\mathbb{Z}^d_{(k)}$. If $\lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) = \lambda(\mathcal{Z})$ exists, then we say that the *probability*

that $g(x) \in \mathcal{Z}$ with x a random d-dimensional integer vector is $\lambda(\mathcal{Z})$. If this is the case, then $\lambda(\mathcal{Z}) \in [0,1]$ since $\lambda^{(k)}(\mathcal{Z}) \in [0,1]$ for all k.

(ii) We define similarly the gcd distribution over the ring of integers mod p^s: for prime p and positive integer s, we denote by $\lambda_{p^s}^{(k)}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \pmod{p^s}$ (up to multiplication by a unit) with x uniformly distributed over $\mathbb{Z}_{(k)}^d$, and by $\lambda_{p^s}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \pmod{p^s}$ (up to multiplication by a unit) with x uniformly distributed over $(\mathbb{Z}/p^s\mathbb{Z})^d$.

More generally, for a finite set $\mathcal{P}$ of prime and positive integer pairs (p,s) (with p a prime and s a positive integer), we denote

$$P_{\mathcal{P}} := \prod_{(p,s)\in\mathcal{P}} p^s$$

and by $\lambda_{P_{\mathcal{P}}}^{(k)}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$ (up to multiplication by a unit) with x uniformly distributed over $\mathbb{Z}_{(k)}^d$, and by $\lambda_{P_{\mathcal{P}}}(\mathcal{Z})$ the probability that $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$ (up to multiplication by a unit) with x uniformly distributed over $(\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z})^d$. Note that $\lambda_{P_{\mathcal{P}}}(\mathcal{Z})$ is the number of solutions to $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$ (up to multiplication by a unit) divided by $P_{\mathcal{P}}^d$. The situation discussed in the previous paragraph is the special case that $\mathcal{P}$ consists of only one element (p,s) and $P_{\mathcal{P}} = p^s$.

(iii) The above definitions also extend to the distribution of multi-gcds. Suppose that $\mathcal{U} = \{U_i\}_{i=1}^w$ is a collection of w nonempty subsets U_i of $\{F_1, F_2, \ldots, F_h\}$. Let

$$g_i(x) := \gcd\left(F(x) : F \in U_i\right), \quad x \in \mathbb{Z}^d \tag{2.1}$$

and

$$g(x) := (g_1, g_2, \ldots, g_w)(x) \in \mathbb{Z}^w,$$

then we adopt the above definitions of functions $\lambda^{(k)}$, λ, $\lambda_{P_{\mathcal{P}}}^{(k)}$ and $\lambda_{P_{\mathcal{P}}}$ for $\mathcal{Z} \subseteq \mathbb{Z}^d$ with only one slight modification: replace "up to multiplication by a unit" with "up to multiplication of the components of g by units".

For convenience, we shall always assume that the notion $g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}}}$ implies the *equivalence of multiplication of its components by units* and that the random vector x is *uniformly distributed* on its range (if known, e.g., $\mathbb{Z}_{(k)}^d$ or $(\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z})^d$).

Remark 2.2. The density $\lambda_p(\cdot)$ defined above in Definition 2.1 (ii) is consistent with the normalized *Haar measure* on $\mathbb{Z}_p^d$, as in [15].

In this section, we establish the properties of $\lambda_{P_{\mathcal{P}}}$ and λ, the existence of λ, and a connection between λ and the λ_{p^s}'s. Then we apply these results to determine the probability that the polynomial values are relatively prime.

2.1. Multi-gcd Distribution over $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$.

We show that the density $\lambda_{P_{\mathcal{P}}}^{(k)}(\cdot)$ over $\mathbb{Z}_{(k)}^d$ (defined above in Definition 2.1) converges to the density $\lambda_{P_{\mathcal{P}}}(\cdot)$ over $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$ as $k \to \infty$, and that $\lambda_{P_{\mathcal{P}}}(\cdot)$ equals $\prod_{(p,s)\in\mathcal{P}} \lambda_{p^s}(\cdot)$.

Theorem 2.3. *For any $\mathcal{Z} \subseteq \mathbb{Z}^w$, we have*

$$\lambda_{P_{\mathcal{P}}}(\mathcal{Z}) = \sum_{z \in \mathcal{Z} \,(\mathrm{mod}\, P_{\mathcal{P}})} \lambda_{P_{\mathcal{P}}}(\{z\}) \tag{2.2}$$

and

$$\lim_{k\to\infty} \lambda_{P_{\mathcal{P}}}^{(k)}(\mathcal{Z}) = \lambda_{P_{\mathcal{P}}}(\mathcal{Z}) = \prod_{(p,s)\in\mathcal{P}} \lambda_{p^s}(\mathcal{Z})\,. \tag{2.3}$$

Proof. (1) The first equality (2.2) follows directly from Definition 2.1.

(2) For the second equality of (2.3), we let $N_{P_\mathcal{P}}(\mathcal{Z})$ be the number of $x \in (\mathbb{Z}/P_\mathcal{P}\mathbb{Z})^d$ for which $g(x) \in \mathcal{Z} \pmod{P_\mathcal{P}}$. The Chinese remainder theorem along with Definition 2.1 then gives

$$P_\mathcal{P}^d \, \lambda_{P_\mathcal{P}}(\mathcal{Z}) = N_{P_\mathcal{P}}(\mathcal{Z}) = \prod_{(p,s)\in\mathcal{P}} N_{p^s}(\mathcal{Z}) = \prod_{(p,s)\in\mathcal{P}} p^{sd} \lambda_{p^s}(\mathcal{Z}) = P_\mathcal{P}^d \prod_{(p,s)\in\mathcal{P}} \lambda_{p^s}(\mathcal{Z}) \,.$$

Dividing both sides by $P_\mathcal{P}^d$ leads to the desired equality.

(3) For the first equality of (2.3), we first observe that if $p \,|\, 2k+1$, then $\lambda_{P_\mathcal{P}}^{(k)}(\mathcal{Z}) = \lambda_{P_\mathcal{P}}(\mathcal{Z})$ by definition. If $p \nmid 2k+1$, then we proceed by approximating $2k+1$ by a multiple of $P_\mathcal{P}$ and estimating $\lambda_{P_\mathcal{P}}^{(k)}(\mathcal{Z})$ using $\lambda_{P_\mathcal{P}}(\mathcal{Z})$.

Let $k \in \mathbb{Z}$ such that $K := 2k+1 \geq P_\mathcal{P}$, then there exists $q \in \mathbb{Z}_+$ such that

$$q \cdot P_\mathcal{P} \leq K < (q+1) \cdot P_\mathcal{P} \,. \tag{2.4}$$

It follows that for any integer y, there are either q or $q+1$ numbers among $\mathbb{Z}_{(k)}$ that equal y mod $P_\mathcal{P}$. Thus the number of $x \in \mathbb{Z}_{(k)}^d$ for which for which $g(x) \in \mathcal{Z} \pmod{P_\mathcal{P}}$ is between $q^d N'$ and $(q+1)^d N'$, where $N' := N_{P_\mathcal{P}}(\mathcal{Z})$, therefore

$$\lambda_{P_\mathcal{P}}^{(k)}(\mathcal{Z}) \in \left[\frac{q^d N'}{K^d} \,, \frac{(q+1)^d N'}{K^d} \right] := J_k \,.$$

Thanks to (2.4), we have

$$J_k \subseteq \left[\frac{q^d N'}{[(q+1)P_\mathcal{P}]^d} \,, \frac{(q+1)^d N'}{(qP_\mathcal{P})^d} \right] = \left[\left(\frac{q}{q+1} \right)^d \frac{N'}{P_\mathcal{P}^d} \,, \left(\frac{q+1}{q} \right)^d \frac{N'}{P_\mathcal{P}^d} \right] ,$$

whose left and right endpoints both converge to $N'/P_\mathcal{P}^d$ as $q \to \infty$. Hence

$$\lambda_{P_\mathcal{P}}^{(k)}(\mathcal{Z}) \to N'/P_\mathcal{P}^d = \lambda_{P_\mathcal{P}}(\mathcal{Z}) \,,$$

as $q \to \infty$, or equivalently, as $k \to \infty$, as desired. □

2.2. **Multi-gcd Distribution over $\mathbb{Z}$.**

We show some properties of the density λ of set unions, subtractions and complements. They will be very useful in determining the value of λ for specific sets (such as in Remark 2.9 (iii)).

Theorem 2.4. *Suppose that $\{\mathcal{Z}_\alpha\}_{\alpha\in\mathcal{A}}$ are pairwise disjoint subsets of $\mathbb{Z}^w$ such that $\lambda(\mathcal{Z}_\alpha)$ exists for all $\alpha \in \mathcal{A}$. If $\mathcal{A}$ is a finite set, then*

$$\lambda\left(\cup_{\alpha\in\mathcal{A}} \mathcal{Z}_\alpha\right) = \sum_{\alpha\in\mathcal{A}} \lambda(\mathcal{Z}_\alpha) \,.$$

Proof. By Definition 2.1, we have

$$\sum_{\alpha\in\mathcal{A}} \lambda(\mathcal{Z}_\alpha) = \sum_{\alpha\in\mathcal{A}} \lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}_\alpha) = \lim_{k\to\infty} \sum_{\alpha\in\mathcal{A}} \lambda^{(k)}(\mathcal{Z}_\alpha) = \lim_{k\to\infty} \lambda^{(k)}\left(\cup_{\alpha\in A} \mathcal{Z}_\alpha\right)$$

and the conclusion follows. □

Theorem 2.5. *Suppose that $\mathcal{Z}' \subseteq \mathcal{Z} \subseteq \mathbb{Z}^w$ such that $\lambda(\mathcal{Z}')$ and $\lambda(\mathcal{Z})$ both exist, then*

$$\lambda(\mathcal{Z} \setminus \mathcal{Z}') = \lambda(\mathcal{Z}) - \lambda(\mathcal{Z}') \,.$$

In particular, for the complement $\mathcal{Z}^c$ of $\mathcal{Z}$ in $\mathbb{Z}^w$, we have

$$\lambda(\mathcal{Z}^c) = 1 - \lambda(\mathcal{Z}) \,.$$

Proof. By Definition 2.1, we have

$$\lambda(\mathcal{Z}) - \lambda(\mathcal{Z}') = \lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) - \lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}') = \lim_{k\to\infty} \left(\lambda^{(k)}(\mathcal{Z}) - \lambda^{(k)}(\mathcal{Z}')\right) = \lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z} \setminus \mathcal{Z}')$$

and the conclusion follows. □

Theorem 2.6. *Suppose that $\mathcal{Y} \in \mathbb{Z}^w$ such that $\lambda(\mathcal{Y}) = 0$, then for any $\mathcal{Z} \subseteq \mathcal{Y}$, we have $\lambda(\mathcal{Z}) = 0$ as well.*

Proof. Since $\lambda^{(k)}(\mathcal{Z}) \geq 0$, $\mathcal{Z} \subseteq \mathcal{Y}$ and $\lim_{k\to\infty} \lambda^{(k)}(\mathcal{Y}) = \lambda(\mathcal{Y}) = 0$, we obtain

$$0 \leq \liminf_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) \leq \limsup_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) \leq \limsup_{k\to\infty} \lambda^{(k)}(\mathcal{Y}) = \lambda(\mathcal{Y}) = 0\,.$$

Therefore

$$\lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) = 0\,,$$

as desired. □

2.3. **Connection between λ and λ_{p^s}.**

We show that the density λ exists and in fact, equals the product of some λ_{p^s}'s.

Assumption 2.7. For all $1 \leq i \leq w$, we have

$$\gcd(F_1, F_2, \ldots, F_h) = \gcd\left(F : F \in U_i\right) = 1 \text{ in } \mathbb{Q}[x_1, x_2, \ldots, x_d]\,.$$

Theorem 2.8. *Suppose that Assumption 2.7 holds. Given positive integers $r \leq w$ and y_i, $1 \leq i \leq r$, let $y = \prod_{j=1}^{\infty} p_j^{s_j}$ with p_j the j-th smallest prime and s_j nonnegative integers, $j = 1, 2, \ldots$ such that $y_i \,|\, y$ for all $1 \leq i \leq r$, then the probability $\lambda(\mathcal{Z})$ exists for*

$$\mathcal{Z} = \left\{(z_1, z_2, \ldots, z_w) \in \mathbb{Z}_+^w : \ z_i = y_i\,,\ \forall\ i \leq r\right\}, \tag{2.5}$$

and in fact

$$\lambda(\mathcal{Z}) = \prod_{j=1}^{\infty} \lambda_{p_j^{s_j+1}}(\mathcal{Z})\,. \tag{2.6}$$

Remark 2.9. (i) The right-hand side of (2.6) is well-defined since $\lambda_{p^s}(\cdot) \in [0, 1]$ for all p and s.

(ii) The special case that all s_j's are either 0 or 1 follows from [6, Theorem 2.3].

(iii) We have assumed that the y_i's are positive. In fact, in the case that $y_i = 0$ for some i, we have $\lambda(\mathcal{Z}) = 0$ on the strength of Theorem 2.6 and that the probability that a nonzero polynomial at a random integer vector equals zero is 0 (see Theorem 2.15 (ii) below).

To prove Theorem 2.8, we need Theorem 2.3 and the following two lemmas.

Lemma 2.10. ([14, Lemma 5.1] or [15, Lemma 21]) *Suppose that $F, G \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ are relatively prime as elements of $\mathbb{Q}[x_1, x_2, \ldots, x_d]$. Let $\nu_\ell^{(k)}$ be the probability that $p \,|\, F(x), G(x)$ for some prime $p > \ell$ with x uniformly distributed over $\mathbb{Z}_{(k)}^d$, i.e.,*

$$\nu_\ell^{(k)} := \#\left\{x \in \mathbb{Z}_{(k)}^d : \ \exists \text{ prime } p > \ell \text{ s.t. } p \,|\, F(x), G(x)\right\} / (2k+1)^d.$$

Then

$$\lim_{\ell\to\infty} \limsup_{k\to\infty} \nu_\ell^{(k)} = 0\,.$$

Lemma 2.11. *Suppose that $G_1, \ldots, G_h \in \mathbb{Q}[x_1, x_2, \ldots, x_d]$ ($h \geq 2$) are relatively prime, then there exists $v = (v_3, \ldots, v_h) \in \mathbb{Z}^{h-2}$ such that*

$$\gcd\left(G_1, G_2 + \sum_{i=3}^{h} v_i G_i\right) = 1.$$

Proof. We prove by induction on h. The case $h = 2$ is trivial since $\gcd(G_1, G_2) = 1$.

Base case: $h = 3$.

We prove by contradiction. Assume the contrary that

$$\gcd(G_1, G_2 + z\,G_3) \neq 1, \quad \forall\ z \in \mathbb{Z}\,.$$

Suppose that the polynomial factorization of G_1 is $\phi_1\phi_2\cdots\phi_u$, then each $G_2 + z\,G_3$ is a multiple of some factor $\phi_{u(z)}$ of G_1 $(1 \leq u(z) \leq u)$. Since there are infinitely many z's, by the pigeonhole principle, at least two of the $u(z)$'s are the same, say $u(z) = u(z')\,(z \neq z')$. Then

$$\phi_{u(z)} \,|\, (G_2 + z\,G_3) - (G_2 + z'G_3) = (z - z')\,G_3$$

thus $\phi_{u(z)} \,|\, G_3$ and hence $\phi_{u(z)} \,|\, (G_2 + z\,G_3) - z\,G_3 = G_2$. Recall that $\phi_{u(z)} \,|\, G_1$ as well. This contradicts with the condition that G_1, G_2 and G_3 are relatively prime.

Inductive step: from $h - 1$ to $h\,(\geq 4)$. Assume that the statement holds for $h - 1$.

Let $H := (G_2, G_3, \ldots, G_h)$ and $H_i := G_i/H\ (2 \leq i \leq h)$, then

$$\gcd(G_1, H) = \gcd(G_1, G_2, \cdots, G_h) = 1 = \gcd(H_2, H_3, \cdots, H_h)\,. \tag{2.7}$$

According to the induction hypothesis for $H_2, H_3, \cdots, H_h$, there exists $v = (v_4, \ldots, v_h) \in \mathbb{Z}^{h-3}$ such that

$$H_3' := H_3 + \sum_{i=4}^{h} v_i H_i \tag{2.8}$$

satisfies

$$\gcd(H_2, H_3') = 1.$$

Combining with (2.7) gives

$$\gcd(G_1, G_2, H_3'H) = \gcd(G_1, H_2H, H_3'H) = \gcd(G_1, \gcd(H_2H, H_3'H)) = \gcd(G_1, H) = 1.$$

Thus we can apply the base case $h = 3$ to $G_1, G_2, H_3'H$ to get an integer z such that

$$\gcd(G_1, G_2 + zH_3'H) = 1.$$

Finally, we represent $H_3'H$ back to a linear combination of the G_i's with integer coefficients by definition (2.8):

$$H_3'H = H_3H + \sum_{i=4}^{h} v_i H_iH = G_3 + \sum_{i=4}^{h} v_i G_i\,,$$

therefore

$$\gcd\left(G_1, G_2 + z\,G_3 + z\sum_{i=4}^{h} v_i G_i\right) = 1,$$

namely, the statement holds for h with the new $v = (z, zv_4, \ldots, zv_h)$. □

Now we are ready to prove Theorem 2.8.

Proof of Theorem 2.8. Let

$$\mathcal{P}_\ell := \{(p_j, s_j + 1)\}_{j=1}^{\ell}\,, \quad \ell \in \mathbb{Z}_+\,,$$

then Theorem 2.3 gives

$$\lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) = \prod_{j=1}^{\ell} \lambda_{p_j^{s_j+1}}(\mathcal{Z})\,.$$

Since $\lambda_{p_j^{s_j+1}}(\mathcal{Z}) \in [0,1]$ for all j, we can let $\ell \to \infty$:

$$\lim_{\ell\to\infty} \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) = \prod_{j=1}^{\infty} \lambda_{p_j^{s_j+1}}(\mathcal{Z}) = \text{RHS of (2.6)}\,. \tag{2.9}$$

Therefore it suffices to show that

$$\lim_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) = \lim_{\ell\to\infty} \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z})\,. \tag{2.10}$$

Since y is finite, there exists $j^* \in \mathbb{Z}_+$ such that $s_j = 0$ for all $j > j^*$. Let

$$\mathcal{I} = \left\{(z_1, z_2, \ldots, z_w) \in \mathbb{Z}_+^w : z_1 = z_2 = \cdots = z_r = 1\right\}$$

then for any $j > j^*$, the sets $\mathcal{Z}$ and $\mathcal{I}$ are equivalent mod p_j under multiplication of the components by units.

We define for $\ell > j^*$,

$$A(\ell) := \left\{x \in \mathbb{Z}^d : g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}_\ell}}\right\}, \quad A^{(k)}(\ell) := \left\{x \in \mathbb{Z}_{(k)}^d : g(x) \in \mathcal{Z} \pmod{P_{\mathcal{P}_\ell}}\right\},$$

$$A^{(k)} := \left\{x \in \mathbb{Z}_{(k)}^d : g(x) \in \mathcal{Z}\right\} \left(\subseteq A^{(k)}(\ell)\right),$$

and

$$B^{(k)}(\ell) := A^{(k)}(\ell) \setminus A^{(k)},$$

then

$$\lambda^{(k)}(\mathcal{Z}) = \frac{\#A^{(k)}}{K^d}\,, \quad \lambda_{P_{\mathcal{P}_\ell}}^{(k)}(\mathcal{Z}) = \frac{\#A^{(k)}(\ell)}{K^d} = \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d} \tag{2.11}$$

with $K := 2k+1$. Therefore

$$\lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) = \lim_{k\to\infty} \lambda_{P_{\mathcal{P}_\ell}}^{(k)}(\mathcal{Z}) = \lim_{k\to\infty} \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d}\,. \tag{2.12}$$

Combining with the first equation in (2.11) leads to

$$\limsup_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) \le \limsup_{k\to\infty} \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d} = \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z})$$

and

$$\liminf_{k\to\infty} \lambda^{(k)}(\mathcal{Z}) \ge \liminf_{k\to\infty} \frac{\#A^{(k)} + \#B^{(k)}(\ell)}{K^d} - \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d} \ge \lambda_{P_{\mathcal{P}_\ell}}(\mathcal{Z}) - \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d}\,.$$

Once we show that

$$\lim_{\ell\to\infty} \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d} = 0\,, \tag{2.13}$$

taking $\ell \to \infty$ in the above two inequalities will yield (2.10).

Now let us prove (2.13). For any $x \in B^{(k)}(\ell)$, there exists $j > \ell\,(> j^*)$ such that $g(x) \notin \mathcal{I} \pmod{p_j^{s_j+1} = p_j}$ (recall that $\mathcal{Z}$ and $\mathcal{I}$ are equivalent). Hence $p_j \mid g_\eta(x)$ for some $\eta \le r$.

Recall that g_η is the gcd of some relatively prime F_i's. If two or more F_i's are involved, then applying Lemma 2.11 to these F_i's leads to two relatively prime linear combinations $\mathcal{G}_\eta$ and $\mathcal{H}_\eta$ of these F_i's with integer coefficients. If there is only one F_i involved, then it must be a constant since the gcd of itself is 1 in $\mathbb{Q}[x_1, x_2, \ldots, x_d]$. In this case, we take $\mathcal{G}_\eta = \mathcal{H}_\eta = F_i$ so that $\gcd(\mathcal{G}_\eta, \mathcal{H}_\eta) = 1$ still holds.

Since $p_j \mid g_\eta(x)$, we have $p_j \,\big|\, \mathcal{G}_\eta(x), \mathcal{H}_\eta(x)$. Hence

$$B^{(k)}(\ell) \subseteq \bigcup_{\eta=1}^{r} \overline{B}_\eta^{(k)}(\ell)\,, \tag{2.14}$$

where

$$\overline{B}_\eta^{(k)}(\ell) := \left\{ x \in \mathbb{Z}_{(k)}^d : \exists\ j > \ell \ \text{ s.t. } \ p_j \,\middle|\, \mathcal{G}_\eta(x)\,, \mathcal{H}_\eta(x) \right\}\,.$$

Applying Lemma 2.10 to $\mathcal{G}_\eta$ and $\mathcal{H}_\eta$ gives

$$\lim_{\ell\to\infty} \limsup_{k\to\infty} \frac{\#\overline{B}_\eta^{(k)}(\ell)}{K^d} = 0\,, \quad \forall\ \eta\,.$$

Combining with (2.14), we obtain

$$\limsup_{\ell\to\infty} \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d} \le \limsup_{\ell\to\infty} \limsup_{k\to\infty} \sum_{\eta=1}^{r} \frac{\#\overline{B}_\eta^{(k)}(\ell)}{K^d} \le \sum_{\eta=1}^{r} \limsup_{\ell\to\infty} \limsup_{k\to\infty} \frac{\#\overline{B}_\eta^{(k)}(\ell)}{K^d} = 0\,.$$

On the other hand, since $\#B^{(k)}(\ell) \ge 0$, we have

$$\liminf_{\ell\to\infty} \limsup_{k\to\infty} \frac{\#B^{(k)}(\ell)}{K^d} \ge 0\,.$$

Hence (2.13) indeed holds. □

2.4. **Relatively Prime Polynomial Values.**

An interesting application of Theorem 2.8 is to determine the probability that the polynomial values are relatively prime.

Theorem 2.12. *Let $w = 1$ and $U_1 = \{\{F_1, F_2, \dots, F_h\}\}$ in Definition 2.1.*
(a) *If $F_1, F_2, \dots, F_h$ are not relatively prime in $\mathbb{Q}[x_1, x_2, \dots, x_d]$, then $\lambda(\{1\}) = 0$;*
(b) *If $F_1, F_2, \dots, F_h$ are relatively prime, i.e.,*

$$\gcd(F_1, F_2, \dots, F_h) = 1 \ \text{ in } \mathbb{Q}[x_1, x_2, \dots, x_d]\,. \tag{2.15}$$

then we have
(i) *$\lambda(\{1\})$ exists and*

$$\lambda(\{1\}) = \prod_p \lambda_p(\{1\})\,;$$

(ii) *the asymptotic result*

$$\lambda_p(\{0\}) = O(p^{-2})\,; \tag{2.16}$$

(iii) *$\lambda(\{1\}) = 0$ if and only if $\lambda_p(\{1\}) = 0$ for some prime p, i.e., if and only if there exists a prime p such that $F_1(x), F_2(x), \dots, F_h(x)$ are multiples of p for all x; in words, the probability that the values of relatively prime polynomials at a random integer are relatively prime is 0 if and only if there exists a prime p such that these polynomials are all always multiples of p.*

Remark 2.13. Theorem 2.12 (b)(ii) and Lemma 2.14 in the proof below are special cases of the Lang-Weil bound [11, Theorem 1]. We present a considerably simpler and more approachable proof. As mentioned in Remark 2.9 and [15, Remark of Lemma 21], Theorem 2.12 (b)(i) follows from [6, Theorem 2.3]; whereas its special case $h = 2$ was shown in [14, Theorem 3.1].

Proof. (a) Let $G = \gcd(F_1, F_2, \dots, F_h)$, then G is a non-constant polynomial. If the gcd $g(x) = 1$, then $G(x) = \pm 1$. Thus $\lambda^{(k)}(\{1\}) \le \sigma_{G=1}^{(k)} + \sigma_{G=-1}^{(k)} \to 0$ as $k \to \infty$ on the strength of Theorem 2.15 (ii), where $\sigma_{G=c}^{(k)}$ ($c = \pm 1$) is the probability that $G(x) = c$ with x uniformly distributed over $\mathbb{Z}_{(k)}^d$. Hence $\lambda(\{1\}) = 0$.

(b) (i) follows directly from Theorem 2.8. For (ii), we prove by induction on d. First, we notice the following facts:

1. If $h = 1$, then F_1 must be a constant due to Assumption (2.15). Hence $\lambda_p(\{0\}) = 0$ for all $p > |F_1|$ and (2.16) follows.

2. If $h \geq 2$, by Lemma 2.11, there exist two linear combinations G and H of the F_i's with integer coefficients such that $\gcd(G, H) = 1$ in $\mathbb{Q}[x_1, x_2, \ldots, x_d]$. Then $p \,|\, g(x)$ implies that $p \,|\, \gcd(G(x), H(x))$, so it suffices to prove for the case $h = 2$.

3. Assume that $h = 2$. Let L be the greatest total degree of the F_i's. If $L = 0$, then F_1, F_2 and thus g are nonzero constants. Thus $\sigma_p = 0$ for any $p > |g|$ and (2.16) follows, so we only need to prove for $L \geq 1$.

Base case: $d = 1$. Assume that $h = 2$.

Thanks to Assumption (2.15), there exist $H_1, H_2 \in \mathbb{Z}[x_1]$ such that $H_1F_1 + H_2F_2 = C$ with C a positive integer constant. If $p \,|\, g(x)$, then $p \,|\, C$ as well. Hence $\sigma_p = 0$ for all $p > C$ and (2.16) follows.

Inductive step: from $d-1$ to $d\,(\geq 2)$. Assume that the statement holds for $d-1$ and that $h = 2$ and $L \geq 1$.

Since $L \geq 1$, without loss of generality, we can assume that F_1 is not a constant and x_1 appears in F_1. We recast F_i as a univariate polynomial $G_i \in (\mathbb{Z}[x_2, \ldots, x_d])[x_1]$ of degree L_i, $i = 1, 2$, then $L_1 \geq 1$. Let $\gamma_{i,j} \in \mathbb{Z}[x_2, \ldots, x_d]\,(0 \leq j \leq L_i)$ be the coefficients of x_1^j in G_i.

Since F_1 and F_2 are relatively prime in $\mathbb{Q}[x_1, x_2, \ldots, x_d]$ by Assumption (2.15), we have

$$\gcd\left(\gamma_{i,j} : 1 \leq i \leq 2\,, 0 \leq j \leq L_i\right) = 1 = \gcd(G_1, G_2) \ \text{ in } (\mathbb{Q}[x_2, \ldots, x_d])[x_1]\,.$$

As a result, there exist $H_1, H_2 \in (\mathbb{Z}[x_2, \ldots, x_d])[x_1]$ and $H_3 \in \mathbb{Z}[x_2, \ldots, x_d]$ such that $H_1G_1 + H_2G_2 = H_3$ and $(H_1, H_2, H_3) = 1$ in $\mathbb{Q}[x_1, x_2, \ldots, x_d]$.

If $p \,|\, g(x)$, then $p \,|\, (G_i(x_2, \ldots, x_d))\,(x_1)\,(\forall\ i), H_3(x_2, \ldots, x_d)$ and either
(1) $p \,|\, \gamma_{i,j}(x_2, \ldots, x_d)$ for all i and j; or
(2) $p \nmid \gamma_{i,j}(x_2, \ldots, x_d)$ for some i, j.

Case (1). Recall that $L_1 \geq 1$. By the induction hypothesis for the at least two polynomials: $\gamma_{i,j}(x_2, \ldots, x_d)\,(1 \leq i \leq 2\,, 0 \leq j \leq L_i)$, the probability that Case (1) happens with $(x_2, \ldots, x_d)$ uniformly distributed on $(\mathbb{Z}/p\mathbb{Z})^{d-1}$ is $O(p^{-2})$.

Case (2). We need the following asymptotic result.

Lemma 2.14. *Let $G \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ be a nonzero polynomial, p a prime, and σ_p the probability that $p \,|\, G(x)$ with x uniformly distributed over $(\mathbb{Z}/p\mathbb{Z})^d$, then we have*

$$\sigma_p = O(p^{-1})\,. \tag{2.17}$$

Proof. Let L be the total degree of G. If $L = 0$, then G is a nonzero constant. For any prime $p > G$, we have $\sigma_p = 0$, thus (2.17) holds.

Now we assume that $L \geq 1$. We prove by induction on d.

Base case: $d = 1$.

Since the number of roots of G mod p is at most L, we get $\sigma_p \leq L/p$ and hence (2.17).

Inductive step: from $d-1$ to $d\,(\geq 2)$. Assume that the statement holds for $d-1$.

We recast G as a univariate polynomial $G_1 \in (\mathbb{Z}[x_2, x_3, \ldots, x_d])[x_1]$. Let $\gamma_1 \in \mathbb{Z}[x_2 \ldots, x_d]$ be the leading coefficient of G_1. Observe that the total degree of G_1 is at most L. If $\gamma_1(x_2, \ldots, x_d) \not\equiv 0 \pmod{p}$, then the probability that $p \,|\, G_1(x_1)$ with x_1 uniformly distributed over $\mathbb{Z}/p\mathbb{Z}$ is no greater than L/p, according to the base case $d = 1$. On the other hand, the probability that $p \,|\, \gamma_1(x_2, \ldots, x_d)$ with $(x_2, \ldots, x_d)$ uniformly distributed over $(\mathbb{Z}/p\mathbb{Z})^{d-1}$ is $O(p^{-1})$ by the induction hypothesis for γ_1. Combining these two cases, we conclude that the probability that $p \,|\, G(x_1, x_2, \ldots, x_d)$ with $(x_1, x_2, \ldots, x_d)$ uniformly distributed over $(\mathbb{Z}/p\mathbb{Z})^d$ is at most $L/p + O(p^{-1}) = O(p^{-1})$. Hence the statement holds for d, as desired. □

Now we go back to the proof of Theorem 2.12 (b)(ii). Thanks to Lemma 2.14, the probability that $p \,|\, H_3(x_2, \ldots, x_d)$ with $(x_2, \ldots, x_d)$ uniformly distributed on $(\mathbb{Z}/p\mathbb{Z})^{d-1}$ is $O(p^{-1})$; moreover, for each $(x_2, \ldots, x_d)$ that satisfies $p \nmid \gamma_{i,j}(x_2, \ldots, x_d)$ for some i, j, the probability that $p \,|\, (G_i(x_2, \ldots, x_d))(x_1)$ with x_1 uniformly distributed on $\mathbb{Z}/p\mathbb{Z}$ is $O(p^{-1})$. Hence the probability that Case (2) happens with $(x_1, x_2, \ldots, x_d)$ uniformly distributed on $(\mathbb{Z}/p\mathbb{Z})^d$ is $(O(p^{-1}))^2 = O(p^{-2})$.

Combining Cases (1) and (2), we conclude that the statement holds for d as well, as desired.

(iii) If $\lambda_p(\{1\}) = 0$ for some prime p, then $\lambda(\{1\}) = 0$ by (i).

Now assume that $\lambda_p(\{1\}) > 0$ for all prime p. On the strength of (ii), there exist a positive constant c and a positive integer j^* such that

$$p_{j^*} > 1 + c > \sqrt{c}\,, \quad \lambda_{p_j}(\{0\}) \le c\, p_j^{-2}\,, \quad \forall\ j \ge j^*.$$

Thus

$$\prod_{j=j^*}^{\infty} \big(1 - \lambda_{p_j}(\{0\})\big) \ge \prod_{j=j^*}^{\infty} \left(1 - \frac{c}{p_j^2}\right) \ge 1 - \sum_{j=j^*}^{\infty} \frac{c}{p_j^2} \ge 1 - \sum_{i=p_{j^*}}^{\infty} \frac{c}{i^2}$$

$$\ge 1 - \sum_{i=p_{j^*}}^{\infty} c\left(\frac{1}{i-1} - \frac{1}{i}\right) = 1 - \frac{c}{p_{j^*} - 1} > 0\,,$$

where in the second inequality, we take advantage of the well-known inequality:

$$(1 - \delta_1)(1 - \delta_2) \cdots (1 - \delta_u) \ge 1 - \delta_1 - \delta_2 - \cdots - \delta_u \tag{2.18}$$

for $\delta_1, \delta_2, \ldots, \delta_u \in [0, 1]$, which can be proved easily by induction on u (base cases: $u = 1, 2$; inductive step from u to $u+1$: $(1-\delta_1)(1-\delta_2)\cdots(1-\delta_{u+1}) \ge (1-\delta_1)(1-\delta_2-\cdots-\delta_{u+1}) \ge 1-\delta_1-\delta_2-\cdots-\delta_{u+1}$).

Hence

$$\prod_p \lambda_p(\{1\}) = \prod_{j=1}^{j^*-1} \lambda_{p_j}(\{1\}) \cdot \prod_{j=j^*}^{\infty} \big(1 - \lambda_{p_j}(\{0\})\big) > 0\,.$$

□

2.5. **Zero Polynomial Values.**

Remark 2.9 (iii) used a well-known result that the probability that a nonzero polynomial at a random integer vector equals zero is 0 ([14, Lemma 4.1]). We conclude this section with a different proof by estimating this probability from above by σ_p and applying Lemma 2.14.

Theorem 2.15. *Let $G \in \mathbb{Z}[x_1, x_2, \ldots, x_d]$ be a nonzero polynomial, p a prime, $\sigma_p^{(k)}$ the probability that $p \,|\, G(x)$ with x uniformly distributed over $\mathbb{Z}_{(k)}^d$, and σ_p the probability that $p \,|\, G(x)$ with x uniformly distributed over $(\mathbb{Z}/p\mathbb{Z})^d$, then*
(i) *we have*

$$\sigma_p^{(k)} \to \sigma_p \ \text{ as } \ k \to \infty\,, \quad \text{and} \quad \sigma_p^{(k)} \le 2^d \sigma_p\,,\ \forall\ k > (p-1)/2\,;$$

(ii) *the probability $\sigma^{(k)}$ that $G(x) = 0$ with x uniformly distributed over $\mathbb{Z}_{(k)}^d$ goes to 0 as $k \to \infty$; in words, the probability that a nonzero polynomial at a random integer vector equals zero is 0. As a consequence, for any given integer c, the probability that $G(x) = c$ is either 0 or 1 (consider the polynomial $G(x) - c$).*

Proof. (i) We follow a similar approach as in the proof of the first equality of (2.3). Let $k \in \mathbb{Z}$ such that $K := 2k + 1 > p$. Then there exists $q \in \mathbb{Z}_+$ such that

$$q \cdot P_{\mathcal{P}} \le K < (q+1) \cdot P_{\mathcal{P}}\,. \tag{2.19}$$

It follows that for any integer y, there are either q or $q+1$ numbers among $\mathbb{Z}_{(k)}$ that equal y mod p. Further, the number of $x \in (\mathbb{Z}/p\mathbb{Z})^d$ for which $p \,|\, G(x)$ is $p^d\sigma_p$, thus the number of $x \in \mathbb{Z}_{(k)}^d$ for which $p \,|\, G(x)$ is between $q^d p^d \sigma_p$ and $(q+1)^d p^d \sigma_p$. Therefore

$$\sigma_p^{(k)} \in \left[\frac{q^d p^d \sigma_p}{K^d}, \frac{(q+1)^d p^d \sigma_p}{K^d} \right] := \Sigma_k . \tag{2.20}$$

Thanks to (2.19), we have

$$\Sigma_k \subseteq \left[\frac{q^d p^d \sigma_p}{[(q+1)p]^d}, \frac{(q+1)^d p^d \sigma_p}{(qp)^d} \right] = \left[\left(\frac{q}{q+1} \right)^d \sigma_p, \left(\frac{q+1}{q} \right)^d \sigma_p \right], \tag{2.21}$$

whose left and right endpoints both converge to σ_p as $q \to \infty$. Hence

$$\sigma_p^{(k)} \to \sigma_p, \quad \text{as } q \to \infty, \text{ or equivalently, as } k \to \infty .$$

Additionally, we deduce $\sigma_p^{(k)} \le 2^d \sigma_p$ from (2.20) and (2.21) along with $q \ge 1$.

(ii) The probability $\sigma^{(k)}$ is no greater than $\sigma_p^{(k)}$, which by virtue of (i) and Lemma 2.14, converges to 0 as $p, k \to \infty$ with $k > (p-1)/2$. □

3. SNF Distribution

Let $m \le n$ be two positive integers. We shall define the *density* of SNF of a random $n \times m$ integer matrix as the limit (if exists) of the density of SNF of a random $n \times m$ matrix with entries independent and uniformly distributed over $\mathbb{Z}_{(k)}$ as $k \to \infty$ (see Definition 3.1 below for a precise definition).

If we regard the minors of an $n \times m$ matrix as polynomials of the nm matrix entries with integer coefficients, then the SNF of a matrix is uniquely determined by the values of these polynomials. Specifically, let $x_1, x_2, \ldots, x_{nm}$ be the nm entries of an $n \times m$ matrix, F_j's be the minors of an $n \times m$ matrix as elements in $\mathbb{Z}[x_1, x_2, \ldots, x_{nm}]$, U_i be the set of $i \times i$ minors ($1 \le i \le m$), then the SNF of this matrix is the diagonal matrix whose i-th diagonal entry is 0 if $g_i(x) = 0$ and $g_i(x)/g_{i-1}(x)$ otherwise, where $x = (x_1, x_2, \ldots, x_{nm})$ and $g_i(x)$ is defined in (2.1).

In this spirit, the multi-gcd distribution as well as the results in Sections 2.1–2.3 have analogues for the SNF distribution of a random integer matrix. This section presents these analogues and the next section will use them to compute the density μ for some interesting types of sets.

Conventionally, the SNF is only defined for a nonzero matrix; however, for convenience, we shall define the SNF of a zero matrix to be itself, so that SNF is well-defined for all matrices. This definition does not change the density (if exists) of SNF of a random $n \times m$ integer matrix since the probability of a zero matrix with entries from $\mathbb{Z}_{(k)}$ is $1/(2k+1)^{nm}$, which converges to 0 as $k \to \infty$.

We denote the SNF of an $n \times m$ matrix M by $\mathrm{SNF}(M) = (\mathrm{SNF}(M)_{i,j})_{n \times m}$ and let $\mathbb{S}$ be the set of all candidates for SNF of an $n \times m$ integer matrix, i.e., the set of $n \times m$ diagonal matrices whose diagonal entries $(d_1, d_2, \ldots, d_m)$ are nonnegative integers such that d_{i+1} is a multiple of d_i, $i = 1, 2, \ldots, m-1$.

For ease of notation, we shall always assume that the matrix entries are *independent and uniformly distributed* on its range (if known, e.g., $\mathbb{Z}_{(k)}$ or $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$), and that the notion $\mathrm{SNF}(M) \in \mathcal{S}$ or $\mathrm{SNF}(M) = D \pmod{P_{\mathcal{P}}}$ for some $\mathcal{S} \subseteq \mathbb{S}$, $D \in \mathbb{S}$ and $P_{\mathcal{P}} = \prod_{(p,s)\in\mathcal{P}} p^s \in \mathbb{Z}_+$ implies the *equivalence of multiplication of the entries of M by units* in $\mathbb{Z}/P_{\mathcal{P}}\mathbb{Z}$, thus we can assume for convenience that the entries of $\mathrm{SNF}(M) \pmod{P_{\mathcal{P}}}$ are zero or divisors of $P_{\mathcal{P}}$.

Definition 3.1. (i) For $\mathcal{S} \subseteq \mathbb{S}$, we denote by $\mu^{(k)}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S}$ with entries of M from $\mathbb{Z}_{(k)}$. If $\lim_{k\to\infty} \mu^{(k)}(\mathcal{S}) = \mu(\mathcal{S})$ exists, then we say that the *probability that*

$\mathrm{SNF}(M) \in \mathcal{S}$ *with* M *a random* $n \times m$ *integer matrix* is $\mu(\mathcal{S})$. If this is the case, then $\mu(\mathcal{S}) \in [0,1]$ since $\mu^{(k)}(\mathcal{S}) \in [0,1]$ for all k.

(ii) We define similarly the SNF distribution over the ring of integers mod p^s: for prime p and positive integer s, we denote by $\mu_{p^s}^{(k)}(\mathcal{S})$ the probability that the $\mathrm{SNF}(M) \in \mathcal{S} \pmod{p^s}$ with entries of M from $\mathbb{Z}_{(k)}$, and by $\mu_{p^s}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{p^s}$ with entries of M from $\mathbb{Z}/p^s\mathbb{Z}$.

More generally, for a finite set $\mathcal{P}$ of prime and positive integer pairs (p,s) (with p a prime and s a positive integer), we denote by $\mu_{P_\mathcal{P}}^{(k)}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{P_\mathcal{P}}$ with entries of M from $\mathbb{Z}_{(k)}$, and by $\mu_{P_\mathcal{P}}(\mathcal{S})$ the probability that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{P_\mathcal{P}}$ with entries of M from $\mathbb{Z}/P_\mathcal{P}\mathbb{Z}$. Note that $\mu_{P_\mathcal{P}}(\mathcal{S})$ is the number of matrices M over $P_\mathcal{P}$ such that $\mathrm{SNF}(M) \in \mathcal{S} \pmod{P_\mathcal{P}}$ divided by $P_\mathcal{P}^{nm}$. The situation discussed in the previous paragraph is the special case that $\mathcal{P}$ consists of only one element (p,s) and $P_\mathcal{P} = p^s$.

In this section, we establish a formula for μ_{p^s}, discuss the properties of $\mu_{P_\mathcal{P}}$ and μ, show the existence of μ and represent it as a product of μ_{p^s}'s.

3.1. SNF Distribution over $\mathbb{Z}/P_\mathcal{P}\mathbb{Z}$.

We have the following formula for μ_{p^s} and analogue of Theorem 2.3 for SNFs.

Theorem 3.2. (i) *Given a prime* p*, a positive integer* s *and a sequence of integers* $0 = a_0 \le a_1 \le \cdots \le a_s \le a_{s+1} = m$*, let* $\boldsymbol{a} := (a_1, a_2, \ldots, a_s)$ *and* $D_{\boldsymbol{a}} \in \mathbb{S}$ *be the diagonal matrix with exactly* $(a_i - a_{i-1})$ p^{i-1}*'s, i.e.,* a_i *non-*p^i*-multiples,* $1 \le i \le s$ *on its diagonal. Then we have*

$$\mu_{p^s}(\{D_{\boldsymbol{a}}\}) = p^{-\sum_{i=1}^{s}(n-a_i)(m-a_i)} \cdot \frac{[p,n][p,m]}{[p,n-a_s][p,m-a_s]\prod_{i=1}^{s}[p,a_i-a_{i-1}]}, \tag{3.1}$$

where

$$[p,0] = 1, \quad [p,\ell] := \prod_{j=1}^{\ell}\left(1-p^{-j}\right), \quad \ell \in \mathbb{Z}_+.$$

(ii) *For any* $\mathcal{S} \subseteq \mathbb{S}$*, we have*

$$\mu_{P_\mathcal{P}}(\mathcal{S}) = \sum_{D \in \mathcal{S} \,(\mathrm{mod}\, P_\mathcal{P})} \mu_{P_\mathcal{P}}(\{D\})$$

and

$$\lim_{k\to\infty} \mu_{P_\mathcal{P}}^{(k)} = \mu_{P_\mathcal{P}}(\mathcal{S}) = \prod_{(p,s)\in\mathcal{P}} \mu_{p^s}(\mathcal{S}). \tag{3.2}$$

Proof. (ii) and (iii) are direct applications of Theorem 2.3 to SNFs. For (i), we compute the number of $n \times m$ matrices over $\mathbb{Z}/p^s\mathbb{Z}$ whose SNF is $D_{\boldsymbol{a}}$ by [7, Theorem 1] (or [8, Theorem 2]) and simplify it to

$$p^{\sum_{i=1}^{s}\left[(n+m)a_i - a_i^2\right]} \cdot \frac{\prod_{i=0}^{a_s-1}(1-p^{-n+j})(1-p^{-m+j})}{\prod_{i=0}^{s-1}\prod_{j=1}^{a_{i+1}-a_i}(1-p^{-j})} =: N. \tag{3.3}$$

Thus

$$\mu_{p^s}(\{D_{\boldsymbol{a}}\}) = p^{-snm}N = \text{RHS of (3.1)}.$$

□

Remark 3.3. In the case of $s = 1$, the formula (3.3) gives the number of $n \times m$ matrices over $\mathbb{Z}/p\mathbb{Z}$ of rank a_1 and is consistent with [16, Exercise 1.192(b)]; whereas in the case of $n = m$, a calculation shows that (3.3) is consistent with the results in [9, pp. 233, 236] (their $|\mathrm{Aut}\, H|$ is our N).

3.2. **SNF Distribution over $\mathbb{Z}$.**

The properties of λ of set unions, subtractions and complements in Section 2.2 also carry over to SNFs. They will be useful in determining the value of μ for some specific sets (for instance, the singleton set of the identity matrix as in Section 4.3).

Theorem 3.4. *Suppose that $\{\mathcal{S}_\alpha\}_{\alpha\in\mathcal{A}}$ are pairwise disjoint subsets of $\mathbb{S}$ such that $\mu(\mathcal{S}_\alpha)$ exists for all $\alpha \in \mathcal{A}$. If $\mathcal{A}$ is a finite set, then*

$$\mu\left(\cup_{\alpha\in\mathcal{A}}\mathcal{S}_\alpha\right) = \sum_{\alpha\in\mathcal{A}}\mu(\mathcal{S}_\alpha)\,.$$

Theorem 3.5. *Suppose that $\mathcal{S}' \subseteq \mathcal{S} \subseteq \mathbb{S}$ such that $\mu(\mathcal{S}')$ and $\mu(\mathcal{S})$ both exist, then*

$$\mu(\mathcal{S}\setminus\mathcal{S}') = \mu(\mathcal{S}) - \mu(\mathcal{S}')\,.$$

In particular for the complement $\mathcal{S}^c$ of $\mathcal{S}$ in $\mathbb{S}$, we have

$$\mu(\mathcal{S}^c) = 1 - \mu(\mathcal{S})\,.$$

Theorem 3.6. *Suppose that $\mathcal{T} \in \mathbb{S}$ such that $\mu(\mathcal{T}) = 0$, then for any $\mathcal{S} \subseteq \mathcal{T}$, we also have $\mu(\mathcal{S}) = 0$.*

3.3. **Connection between μ and μ_{p^s}.**

Theorem 2.8 has an analogue for SNFs as well, by virtue of the following well-known lemma (see [3, Theorem 61.1] for an easy proof).

Lemma 3.7. *Fix a positive integer r. The determinant of an $r \times r$ matrix as a polynomial of its r^2 entries $x_1, x_2, \ldots, x_{r^2}$ is irreducible in $\mathbb{Q}[x_1, x_2, \ldots, x_{r^2}]$.*

For any $i \le m \wedge (n-1)$ (i.e., $\min\{m, n-1\}$, which is m if $m < n$, and $n-1$ if $m = n$, recalling that $m \le n$), the set U_i contains at least two different minors, which are both irreducible as polynomials of the entries on the strength of Lemma 3.7 and therefore relatively prime. Hence Assumption 2.7 holds with $w = m \wedge (n-1)$. This allows us to apply Theorem 2.8 to SNFs and obtain the following analogue. In addition, we will compute the density $\mu(\mathcal{S})$ explicitly later in Section 4.1.

Theorem 3.8. *Given positive integers $r \le m \wedge (n-1)$ and $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$, let $z = \prod_{j=1}^{\infty} p_j^{s_j}$ with p_j the j-th smallest prime and s_j nonnegative integers, $j = 1, 2, \ldots$ such that $d_r \,|\, z$, then the probability $\mu(\mathcal{S})$ exists for*

$$\mathcal{S} = \{D := (D_{i,j})_{n\times m} \in \mathbb{S} :\ D_{i,i} = d_i\,,\ \forall\ i \le r\}\,, \tag{3.4}$$

and in fact

$$\mu(\mathcal{S}) = \prod_{j=1}^{\infty}\mu_{p_j^{s_j+1}}(\mathcal{S})\,. \tag{3.5}$$

Remark 3.9. (i) The right-hand side of (3.5) is well-defined since $\mu_{p^s}(\cdot) \in [0,1]$ for all p and s.

(ii) We have assumed that $r \le m \wedge (n-1)$; in fact, we have $\mu(\mathcal{S}) = 0$ otherwise. Recall that $m \le n$ and note that $r \le m$, thus in the case of $r > m \wedge (n-1)$, we must have $r = m = n$. As a result, any matrix M with $\mathrm{SNF}(M) \in \mathcal{S}$ satisfies $|M| = \pm d_n$. We will show later that the probability that the determinant of a random $n \times n$ integer matrix equals $\pm c$ is 0 for all constant c (Theorem 4.5).

(iii) We have also assumed that the d_i's are positive; in fact, we have $\mu(\mathcal{S}) = 0$ otherwise. If $d_i = 0$ for some i, then all $i \times i$ minors of any matrix M with $\mathrm{SNF}(M) \in \mathcal{S}$ are zero. Applying Theorem 4.5 to $c = 0$ yields the desired result.

4. Applications

Now we apply Theorems 3.2 and 3.8 to compute the density μ explicitly for the following subsets of $\mathbb{S}$: matrices with first few diagonal entries given (i.e., with the form of (3.4)), full rank matrices, a finite subset, matrices with diagonal entries all equal to 1, and square matrices with at most $\ell\,(=1,2,\ldots,n)$ diagonal entries not equal to 1.

4.1. **Density of the Set** (3.4)**.**

For the set $\mathcal{S}$ of (3.4), i.e., of matrices with first r diagonal entries given, we take $z = d_r$ in Theorem 3.8, then it suffices to compute $\mu_{p^{s+1}}(\mathcal{S})$ for each $(p,s) = (p_j, s_j)$. In mod p^{s+1}, the set $\mathcal{S}$ has $m-r+1$ elements (see (4.12) below). Further, since formula (3.1) gives the density $\mu_{p^{s+1}}$ of each element of $\mathcal{S}$, one can take the sum over $\mathcal{S}$ to get an expression for $\mu_{p^{s+1}}(\mathcal{S})$ (Theorem 3.2), and compute this sum explicitly when $m-r$ is small, such as in Theorems 4.8 and 4.9 below. However, this sum is hard to compute when $m-r$ is large, for example, when m is large and r is fixed; in this case, we recast $\mathcal{S}$ as the difference between a subset of $\mathbb{S}$ and the union of other $r-1$ subsets such that for each of these r sets, its density $\mu_{p^{s+1}}$ is given directly by (3.1).

We work out two examples to illustrate this idea, and then deal with the general case.

4.1.1. *The First Example: Relatively Prime Entries.*

Our approach reproduces the following result mentioned at the beginning of this paper.

Theorem 4.1. *Let $\mathcal{S}$ be the set of* (3.4) *with $r=1$ and $d_1=1$, then we have*

$$\mu(\mathcal{S}) = \frac{1}{\zeta(nm)}\,, \tag{4.1}$$

where $\zeta(\cdot)$ is the Riemann zeta function.

Proof. Applying Theorem 3.8 with $r=1\,,\ d_1=1$ and $s_j=0\,,\ j=1,2,\ldots$ gives

$$\mu(\mathcal{S}) = \prod_p \mu_p(\mathcal{S})\,, \tag{4.2}$$

therefore it reduces to computing $\mu_p(\mathcal{S})$ for each p.

Recall the equivalence of multiplication by units, therefore we only have two choices for matrix entries in mod p: 1 and 0. The set $\mathcal{S}$ (mod p) consists of all the matrices in $\mathbb{S}$ whose first diagonal entry is 1, thus $\mathcal{S} = \{D_{\boldsymbol{a}} : \boldsymbol{a} = (a_1) \geq 1\}$ (mod p) (recall from Theorem 3.2 that $\boldsymbol{a} := (a_1, a_2, \ldots, a_s)$ and that $D_{\boldsymbol{a}} \in \mathbb{S}$ is the diagonal matrix with exactly a_i non-p^i-multiples on its diagonal). Therefore

$$\mu_p(\mathcal{S}) = 1 - \mu_p(\{D_{(0)}\})\,.$$

We apply (3.1) to get $\mu_p(\{D_{(0)}\}) = p^{-nm}$, thus $\mu_p(\mathcal{S}) = 1 - p^{-nm}$. Plugging into (4.2) along with the Euler product formula

$$\prod_p \left(1-p^{-i}\right) = \frac{1}{\zeta(i)} \in (0,1)\,,\quad \forall\ i \geq 2 \tag{4.3}$$

yields (4.1). □

4.1.2. *Another Example.*

Theorem 4.2. *Let $\mathcal{S}$ be the set of* (3.4) *with $r=2$, $d_1=2$ and $d_2=6$, then we have*

$$\mu(\mathcal{S}) = \mu_{2^2}(\mathcal{S})\,\mu_{3^2}(\mathcal{S}) \prod_{p>3} \mu_p(\mathcal{S})\,, \tag{4.4}$$

where

$$\mu_{2^2}(\mathcal{S}) = 2^{-nm}\left(1 - 2^{-nm} - 2^{-(n-1)(m-1)} \cdot \frac{(1-2^{-n})\,(1-2^{-m})}{1-2^{-1}}\right), \tag{4.5}$$

$$\mu_{3^2}(\mathcal{S}) = 3^{-(n-1)(m-1)}\left(1 - 3^{-(n-1)(m-1)}\right)\frac{(1-3^{-n})\,(1-3^{-m})}{1-3^{-1}}, \tag{4.6}$$

$$\mu_p(\mathcal{S}) = 1 - p^{-nm} - p^{-(n-1)(m-1)} \cdot \frac{(1-p^{-n})\,(1-p^{-m})}{1-p^{-1}} = 1 - \sum_{(n-1)(m-1)}^{(n-1)m} p^{-i} + \sum_{n(m-1)+1}^{nm-1} p^{-i}\,. \tag{4.7}$$

Proof. The first equation (4.4) follows directly from Theorem 3.8 with $r = 2\,,\ d_1 = 2\,,\ d_2 = z = 6\,,$ $s_1 = s_2 = 1\,,\ s_j = 0\,,\ j \geq 3\,.$ Therefore it reduces to calculating $\mu_{p^s}(\mathcal{S})$ for $(p,s) = (2,2)$, $(3,2)$ and $(p,1)$ with $p > 3\,.$

Case 1. $p > 3$ and $s = 1\,.$

Recall the equivalence of multiplication by units, therefore we only have two choices for matrix entries in mod p: 1 and 0. The set $\mathcal{S}\pmod p$ consists of all the matrices in $\mathbb{S}$ whose first two diagonal entries are 1, thus $\mathcal{S} = \{D_{\boldsymbol{a}} : \boldsymbol{a} = (a_1) \geq 2\} \pmod p$ (recall $\boldsymbol{a}$ again from Theorem 3.2). Therefore

$$\mu_p(\mathcal{S}) = 1 - \mu_p(\{D_{(0)}\}) - \mu_p(\{D_{(1)}\})\,.$$

We then apply (3.1) to get $\mu_p(\{D_{(0)}\})$ and $\mu_p(\{D_{(1)}\})$, and (4.7) follows.

Case 2. $p = 2$ and $s = 2\,.$

We have three choices for matrix entries in mod 2^2: 1, 2 and 0. The set $\mathcal{S}\pmod{2^2}$ consists of all the matrices in $\mathbb{S}$ whose first two diagonal entries are 2, thus $\mathcal{S} = \{D_{\boldsymbol{a}=(a_1,a_2)} : a_1 = 0\,,\ a_2 \geq 2\}$ $\pmod{2^2}$. Therefore

$$\mu_{2^2}(\mathcal{S}) = \mu_{2^2}(\{D_{(a_1,a_2)} : a_1 = 0\}) - \mu_{2^2}(\{D_{(0,0)}\}) - \mu_{2^2}(\{D_{(0,1)}\})\,. \tag{4.8}$$

Notice that the set $\{D_{(a_1,a_2)} : a_1 = 0\} \pmod{2^2}$ consists of all the matrices in $\mathbb{S}$ whose diagonal entries are all multiples of 2 (i.e., either 2 or 0); in other words, in mod 2, it contains only one element – the zero matrix. Hence

$$\mu_{2^2}(\{D_{(a_1,a_2)} : a_1 = 0\}) = \mu_2(\{D_{(0)}\})\,.$$

Plugging into (4.8) and applying (3.1) to get $\mu_2(\{D_{(0)}\})$, $\mu_{2^2}(\{D_{(0,0)}\})$ and $\mu_{2^2}(\{D_{(0,1)}\})$, we obtain (4.5).

Case 3. $p = 3$ and $s = 2\,.$

We have three choices for matrix entries in mod 3^2: 1, 3 and 0. The set $\mathcal{S}\pmod{3^2}$ consists of all the matrices in $\mathbb{S}$ whose first two diagonal entries are 1 and 3, respectively, thus $\mathcal{S} = \{D_{\boldsymbol{a}=(a_1,a_2)} :$ $a_1 = 1\,,\ a_2 \geq 2\} \pmod{3^2}$. Therefore

$$\mu_{3^2}(\mathcal{S}) = \mu_{3^2}(\{D_{(a_1,a_2)} : a_1 = 1\}) - \mu_{3^2}(\{D_{(1,1)}\})\,. \tag{4.9}$$

Notice that the set $\{D_{(a_1,a_2)} : a_1 = 1\} \pmod{3^2}$ consists of all the matrices in $\mathbb{S}$ whose first diagonal entry is 1 and all other diagonal entries are multiples of 3 (i.e., either 3 or 0); in other words, in mod 3, it contains only one element – the diagonal matrix whose diagonal entries are $1, 0, 0, \ldots, 0$. Hence

$$\mu_{3^2}(\{D_{(a_1,a_2)} : a_1 = 1\}) = \mu_3(\{D_{(1)}\})\,.$$

Plugging into (4.9) and applying (3.1) to get $\mu_3(\{D_{(1)}\})$ and $\mu_{3^2}(\{D_{(1,1)}\})$, we obtain (4.6). □

4.1.3. *The General Case.*

Theorem 4.3. *Let $\mathcal{S}$ be the set of* (3.4) *in Theorem 3.8 with $d_r = \prod_{j=1}^{\infty} p_j^{s_j}$, then for $(p,s) = (p_j, s_j)$, $j = 1, 2, \ldots$, we have*

$$\mu_{p^{s+1}}(\mathcal{S}) = p^{-\sum_{i=1}^{s}(n-\tilde{a}_i)(m-\tilde{a}_i)} \cdot \frac{[p,n][p,m]}{[p,n-\tilde{a}_s][p,m-\tilde{a}_s]\prod_{i=1}^{s}[p,\tilde{a}_i-\tilde{a}_{i-1}]}$$

$$- \sum_{\ell=\tilde{a}_s}^{r-1} p^{-(n-\ell)(m-\ell)-\sum_{i=1}^{s}(n-\tilde{a}_i)(m-\tilde{a}_i)} \cdot \frac{[p,n][p,m]}{[p,n-\ell][p,m-\ell][p,\ell-\tilde{a}_s]\prod_{i=1}^{s}[p,\tilde{a}_i-\tilde{a}_{i-1}]}, \tag{4.10}$$

where $\tilde{a}_i$ $(0 \le i \le s)$ is the number of non-p^i-multiples among $d_1, d_2, \ldots, d_r$ (thus $\tilde{a}_s \le r-1$). In particular, when $s = 0$ (which holds for all but finitely many j's), we have

$$\mu_p(\mathcal{S}) = 1 - \sum_{\ell=0}^{r-1} p^{-(n-\ell)(m-\ell)} \cdot \frac{[p,n][p,m]}{[p,n-\ell][p,m-\ell][p,\ell]}. \tag{4.11}$$

The value of $\mu(\mathcal{S})$ is then given by Theorem 3.8 with $z = d_r$.

Proof. Recalling from Theorem 3.2 the notation of $D_{\boldsymbol{a}}$, we recast $\mathcal{S}$ as

$$\mathcal{S} = \{D_{\boldsymbol{a}=(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\,,\ a_{s+1} \ge r\} \pmod{p^{s+1}}, \tag{4.12}$$

and therefore

$$\mu_{p^{s+1}}(\mathcal{S}) = \mu_{p^{s+1}}(\{D_{\boldsymbol{a}=(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\}) - \sum_{\ell=\tilde{a}_s}^{r-1} \mu_{p^{s+1}}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s,\ell)}\}). \tag{4.13}$$

Notice that the set $\{D_{\boldsymbol{a}=(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\} \pmod{p^{s+1}}$ in the first term on the right-hand side of (4.13) consists of all the matrices in $\mathbb{S}$ with exactly $\tilde{a}_i$ $(1 \le i \le s)$ non-p^i-multiples on its diagonal; in other words, in mod p^s, it contains only one element – the diagonal matrix with exactly $\tilde{a}_i$ non-p^i-multiples, i.e., $(\tilde{a}_i - \tilde{a}_{i-1})$ p^{i-1}'s, $1 \le i \le s$ on its diagonal. Hence

$$\mu_{p^{s+1}}(\{D_{\boldsymbol{a}=(a_1,a_2,\ldots,a_{s+1})} : a_i = \tilde{a}_i\,,\ 1 \le i \le s\}) = \mu_{p^s}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s)}\}). \tag{4.14}$$

Plugging into (4.13) and applying (3.1) to get $\mu_{p^s}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s)}\})$ and $\mu_{p^{s+1}}(\{D_{(\tilde{a}_1,\tilde{a}_2,\ldots,\tilde{a}_s,\ell)}\})$, $1 \le \ell \le r-1$, we obtain (4.10). □

Remark 4.4. We notice that the density $\mu_{p^s}(\{D_{\boldsymbol{a}}\})$ of (3.1) is a polynomial of p^{-1} with integer coefficients since $m - a_s + \sum_{i=1}^{s}(a_i - a_{i-1}) = m$. The $\mu_p(\mathcal{S})$ of (4.11) is also a polynomial of p^{-1} with integer coefficients and with constant term 1 (see the $\mu_p(\mathcal{S})$ of (4.7) as an example). If we replace each occurrence of p by $p^{\boldsymbol{z}}$, where $\boldsymbol{z}$ is a complex variable, and plug into (3.5) of Theorem 3.8, we get an Euler product for some kind of generalized zeta function.

For instance, when $m = n = 3$, for the set $\mathcal{S}$ in Theorem 4.2, we apply (4.7) to get

$$\mu_p(\mathcal{S}) = 1 - p^{-4} - p^{-5} - p^{-6} + p^{-7} + p^{-8} = \left(1 - p^{-2}\right)\left(1 - p^{-3}\right)\left(1 + p^{-2} + p^{-3}\right).$$

Taking the product over all primes p and applying the Euler product formula (4.3), we obtain

$$\prod_p \mu_p(\mathcal{S}) = \frac{1}{\zeta(2)\zeta(3)} \prod_p \left(1 + p^{-2} + p^{-3}\right).$$

Plugging into (4.4), we see that to obtain the density $\mu(\mathcal{S})$, it reduces to computing $\prod_p(1 + p^{-2} + p^{-3})$, or to understanding the Euler product $\prod_p(1 + p^{-2\boldsymbol{z}} + p^{-3\boldsymbol{z}})$.

It would be interesting to study whether such an Euler product for some generalized zeta function (1) has any interesting properties relevant to SNF; (2) extends to a meromorphic function on all of $\mathbb{C}$; (3) satisfies a functional equation.

4.2. **The Determinant.**

The determinant of an $m \times m$ matrix can be regarded as a polynomial G of its m^2 entries. Note that G is not a constant since it takes values 1 and 0 for the identity matrix and the zero matrix, respectively. Thus we can apply Theorem 2.15 to G and obtain the following.

Theorem 4.5. *Let c be an integer. The probability that the determinant equals c for an $m \times m$ matrix with entries from $\mathbb{Z}_{(k)}$ goes to 0 as $k \to \infty$; in other words, the density of the determinant of a random $m \times m$ integer matrix is always 0.*

This result plays an important role in the next two theorems. The first of them shows that the probability that a random $n \times m$ integer matrix is full rank is 1.

Theorem 4.6. *If $\mathcal{S} \subseteq \mathbb{S}$ satisfies $D_{m,m} = 0$ for all $D = (D_{i,j})_{n\times m} \in \mathcal{S}$, then we have $\mu(\mathcal{S}) = 0$; in other words, the probability that an $n \times m$ matrix with entries from $\mathbb{Z}_{(k)}$ is full rank goes to 1 as $k \to \infty$.*

Proof. If $\mathrm{SNF}(M)_{m,m} = 0$, then all $m \times m$ minors of M are zero. Therefore the result follows from Theorem 4.5 with $c = 0$. □

When $m = n$, we can generalize Theorem 4.6 to $\mathcal{S}$ with finitely many values of $D_{m,m}$'s.

Theorem 4.7. *Suppose that $m = n$ and $\mathcal{S} \subset \mathbb{S}$, then we have $\mu(\mathcal{S}) = 0$ if the set $\{D_{n,n} : D = (D_{i,j})_{n\times n} \in \mathcal{S}\}$ is finite; in particular, this holds for any finite subset $\mathcal{S} \subset \mathbb{S}$.*

Proof. For any M such that $\mathrm{SNF}(M) = D \in \mathcal{S}$, we have $|M| = \pm D_{1,1}D_{2,2}\cdots D_{n,n}$. As a consequence, if $D_{n,n} = 0$, then $|M| = 0$; if $D_{n,n} \neq 0$, then the $D_{i,i}$'s are divisors of $D_{n,n}$ and therefore $|M|$ has finitely many choices. The result then follows from Theorem 4.5. □

If $D_{n,n} \neq 0$ for all $D \in \mathcal{S}$, then we have another proof of Theorem 4.7 without invoking Theorem 4.5. We cannot take advantage of (3.2) from Theorem 3.8 since $r = m = n > m \wedge (n-1)$ in this case. Instead, we will start from the observation that $\mu^{(k)}(\mathcal{S}) \le \mu^{(k)}_{P(\ell)}(\{I\})$ with $P(\ell)$ a product of primes and I the identity matrix, then bound $\mu^{(k)}_{P(\ell)}(\{I\})$ from above by $2^{n^2}\mu_{P(\ell)}(\{I\})$ through a similar idea as in the proof of (2.3) (approximating $2k+1$ by a multiple of $P(\ell)$), and finally show that $\mu_{P(\ell)}(\{I\}) \to 0$ as $\ell \to \infty$.

Another Proof of Theorem 4.7 with $D_{n,n} \neq 0$ for all $D \in \mathcal{S}$. Let I be the $n \times n$ identity matrix and $j^* \in \mathbb{Z}_+$ such that $p_j > c$ for all $j \ge j^*$. Then for any $j > j^*$, $\mathrm{SNF}(M) \in \mathcal{S} \pmod{p_j}$ only if $\mathrm{SNF}(M) = I \pmod{p_j}$.

Applying (3.3) with $s = 1$ and $a_1 = n$ (or [16, Exercise 1.192(b)]), we get the number of $n \times n$ non-singular matrices over $\mathbb{Z}/p_j\mathbb{Z}$:

$$p_j^{n^2}[p_j, n] := \beta_j\,.$$

Set

$$P(\ell) := p_{j^*}\, p_{j^*+1}\cdots p_\ell\,,\ \ell \ge j^*.$$

Then $\mathrm{SNF}(M) \in \mathcal{S} \pmod{P(\ell)}$ only if $\mathrm{SNF}(M) = I \pmod{P(\ell)}$. Hence $\mu^{(k)}_{P(\ell)}(\mathcal{S}) \le \mu^{(k)}_{P(\ell)}(\{I\})$.

By the Chinese remainder theorem, the number of $n \times n$ matrices over $\mathbb{Z}/P(\ell)\mathbb{Z}$ whose SNF equals $I \bmod P(\ell)$ is

$$\beta_{j^*}\beta_{j^*+1}\cdots\beta_\ell = \prod_{j=j^*}^{\ell} p_j^{n^2}[p_j, n] = P(\ell)^{n^2}\prod_{j=j^*}^{\ell}[p_j, n] := \beta(\ell)\,. \tag{4.15}$$

For any integer k with $K := 2k+1 > P(\ell)$, there exists $q \in \mathbb{Z}_+$ such that

$$q \cdot P(\ell) \le K < (q+1)\cdot P(\ell)\,. \tag{4.16}$$

Then for any integer z, there are at most $q+1$ numbers among $\mathbb{Z}_{(k)}$ that equal z mod $P(\ell)$. Therefore the number of $n\times n$ matrices with entries from $\mathbb{Z}_{(k)}$ whose SNF is equal to I mod $P(\ell)$ is at most $(q+1)^{n^2}\beta(\ell)$. Hence

$$\mu^{(k)}_{P(\ell)}(\{I\}) \le \frac{(q+1)^{n^2}\beta(\ell)}{K^{n^2}} \le \frac{(q+1)^{n^2}\beta(\ell)}{[qP(\ell)]^{n^2}} = \left(\frac{q+1}{q}\right)^{n^2}\frac{\beta(\ell)}{P(\ell)^{n^2}} \le 2^{n^2}\prod_{j=j^*}^{\ell}[p_j,n]\,, \tag{4.17}$$

on the strength of (4.16) and (4.15) (note that $P(\ell)^{-n^2}\beta(\ell)=\mu_{P(\ell)}(\{I\})$ by (4.15) and (3.2)).

Notice that

$$1-x\le \exp(-x)\,,\quad \forall\ x\in[0,1]\,. \tag{4.18}$$

(To see this, let $W(x):=1-x-\exp(-x)$, $x\in[0,1]$, then $W'(x)=-1+\exp(-x)\le 0$. Hence $W(x)\le W(0)=0$.)

Applying (4.18) with $x=p_j^{-1}$ ($j^*\le j\le \ell$), we obtain

$$[p_j,n]\le 1-p_j^{-1}\le \exp\left(-p_j^{-1}\right).$$

Plugging into (4.17) yields

$$\mu^{(k)}_{P(\ell)}(\{I\}) \le 2^{n^2}\prod_{1\le j\le \ell}\exp\left(-p_j^{-1}\right) = 2^{n^2}\exp\left(-\sum_{j^*\le j\le\ell}p_j^{-1}\right)\to 0 \quad \text{as}\ \ \ell\to\infty$$

with $2k+1\,(=K)>P(\ell)$, by the well-known result that

$$\sum_{1\le j\le\ell}p_j^{-1}\to\infty \quad \text{as}\ \ \ell\to\infty\,.$$

Since $\mu^{(k)}(\mathcal{S})\le\mu^{(k)}_{P(\ell)}(\mathcal{S})\le\mu^{(k)}_{P(\ell)}(\{I\})$, we deduce that $\mu^{(k)}(\mathcal{S})\to 0$ as $k\to\infty$, as desired. □

4.3. **Probability that All Diagonal Entries of the SNF Are 1.**

Theorem 4.7 (along with Theorem 3.6) implies that the probability that all diagonal entries of an SNF are 1 is 0 if $m=n$; however, as we will see soon, this probability is positive if $m<n$. We will need Theorems 3.2 and 3.8 to determine its value.

Theorem 4.8. *Let E be the $n\times m$ diagonal matrix whose diagonal entries are all 1. If $m<n$, then we have*

$$\mu(\{E\}) = \frac{1}{\prod_{i=n-m+1}^{n}\zeta(i)} \to \begin{cases} 1\,, & \text{if } m \text{ is fixed} \\ \frac{1}{\prod_{i=n-m+1}^{\infty}\zeta(i)}\,, & \text{if } n-m \text{ is fixed}\end{cases},\quad \text{as}\ \ n\to\infty\,.$$

Proof. Apply Theorem 3.8 with $\mathcal{S}=\{E\}$, $r=m$, $d_i=z=1$, $s_j=0$ for all i,j, and then Theorem 3.2 with $s=1$, $a_1=m$:

$$\begin{aligned}\mu(\{E\}) &= \prod_p \mu_p(\{E\}) = \prod_p \frac{[p,n]}{[p,n-m]} = \prod_p\prod_{i=n-m+1}^{n}\left(1-p^{-i}\right) = \prod_{i=n-m+1}^{n}\prod_p\left(1-p^{-i}\right)\\ &= \frac{1}{\prod_{i=n-m+1}^{n}\zeta(i)}\,,\end{aligned}$$

on the strength of $n-m+1\ge 2$ and the Euler product formula (4.3).

Finally, thanks to the fact that $\zeta(i)\downarrow 1$ as $i\to\infty$, we obtain the limits of $\mu(\{E\})$ as desired. □

4.4. **Probability that At Most ℓ Diagonal Entries of the SNF Are Not 1.**

In this section, we assume that $m = n$. We provide a formula for the probability that an SNF has at most ℓ diagonal entries not equal to 1 and a formula for the limit of this probability as $n \to \infty$. In particular, when $\ell = 1$, this limit is the reciprocal of a product of values of the Riemann zeta function at positive integers and equals 0.846936. For bigger ℓ, we prove that this limit converges to 1 as $\ell \to \infty$ and find its asymptotics (see (4.38)).

4.4.1. *Cyclic SNFs ($\ell = 1$).*

We shall say that an SNF is *cyclic* if it has at most one diagonal entry not equal to 1, i.e., if the corresponding cokernel is cyclic. Denote the set of $n \times n$ cyclic SNFs by $\mathcal{T}_n$. We will compute the probability $\mu(\mathcal{T}_n)$ of having a cyclic SNF, and show that this probability strictly decreases to $0.846936\cdots$ as $n \to \infty$. As mentioned above, this result was first obtained by Ekedahl [6, Section 3]. Later Nguyen and Shparlinski [13, (1.2)] showed that if take a subgroup of $\mathbb{Z}^n$ uniformly among all subgroups of index at most V and let $V \to \infty$, then the probability that the quotient group is cyclic is also $\mu(\mathcal{T}_n)$. This result is equivalent to computing the probability that an $n \times n$ integer matrix has a cyclic cokernel using a certain probability distribution different from μ. We do not know a simple reason why these two probability distributions yield the same probability of a cyclic cokernel. Perhaps there is a universality result which gives the same conclusion for a wide class of probability distributions.

Theorem 4.9. *We have*
(i)

$$\mu(\mathcal{T}_n) = \frac{1}{\prod_{i=2}^{n} \zeta(i)} \cdot \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^n}\right) =: Z_n\,; \tag{4.19}$$

(ii) Z_n is strictly decreasing in n;
(iii)

$$Z_2 = \frac{1}{\zeta(4)} = \frac{90}{\pi^4} \approx 0.923938\,;$$

(iv)

$$\lim_{n\to\infty} Z_n = \frac{1}{\zeta(6)\prod_{i=4}^{\infty} \zeta(i)} \approx 0.846936\,.$$

Proof. (i) Apply Theorem 3.8 with $\mathcal{S} = \mathcal{T}_n$, $r = n-1$, $d_i = z = 1$, $s_j = 0$ for all i, j, and then Theorem 3.2 with $s = 1$, $a_1 = n$, $n-1$, respectively:

$$\begin{aligned}\mu(\mathcal{T}_n) &= \prod_p \mu_p(\mathcal{T}_n) = \prod_p \left([p,n] + \frac{p^{-1}[p,n]^2}{[p,1]^2[p,n-1]}\right) = \prod_p \frac{[p,n]}{[p,1]} \left([p,1] + \frac{p^{-1}[p,n]}{[p,1][p,n-1]}\right) \\ &= \frac{1}{\prod_{i=2}^{n} \zeta(i)} \prod_p \left(1 - p^{-1} + \frac{p^{-1}(1-p^{-n})}{1-p^{-1}}\right) = \frac{1}{\prod_{i=2}^{n} \zeta(i)} \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^n}\right) = Z_n\,.\end{aligned} \tag{4.20}$$

Here in the fourth equality we used the fact that

$$\prod_p \frac{[p,n]}{[p,1]} = \prod_p \prod_{i=2}^{n} \left(1 - p^{-i}\right) = \prod_{i=2}^{n} \prod_p \left(1 - p^{-i}\right) = \frac{1}{\prod_{i=2}^{n} \zeta(i)}\,, \tag{4.21}$$

by virtue of the Euler product formula (4.3).

(ii) We consider the ratio:

$$\frac{Z_{n+1}}{Z_n} = \prod_p \left(1 - p^{-(n+1)}\right) \cdot \frac{1 + p^{-2} + p^{-3} + \cdots + p^{-(n+1)}}{1 + p^{-2} + p^{-3} + \cdots + p^{-n}}\,,$$

thus it suffices to show

$$\left(1-p^{-(n+1)}\right)\cdot\frac{1+p^{-2}+p^{-3}+\cdots+p^{-(n+1)}}{1+p^{-2}+p^{-3}+\cdots+p^{-n}}<1 \tag{4.22}$$

for all p. For ease of notation, we denote p^{-1} by t throughout this paper, then

$$\text{LHS of (4.22)}=\left(1-t^{n+1}\right)\cdot\left(1+\frac{t^{n+1}}{1+t^2+t^3+\cdots+t^n}\right)<\left(1-t^{n+1}\right)\left(1+t^{n+1}\right)=1-t^{2(n+1)}<1\,.$$

(iii) When $n=2$, it follows from definition (4.19) that

$$Z_2=\prod_p\left(1-p^{-2}\right)\left(1+p^{-2}\right)=\prod_p\left(1-p^{-4}\right)=\frac{1}{\zeta(4)}\,.$$

(iv) Now assume that $n\geq 3$. According to the definition (4.19) of Z_n, it suffices to prove that

$$\lim_{n\to\infty}\prod_p\left(1+\frac{1}{p^2}+\frac{1}{p^3}+\cdots+\frac{1}{p^n}\right)=\frac{\zeta(2)\zeta(3)}{\zeta(6)}\,.$$

In fact, we will show that

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)}=\prod_p\left(1+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)=\lim_{n\to\infty}\prod_p\left(1+\frac{1}{p^2}+\frac{1}{p^3}+\cdots+\frac{1}{p^n}\right). \tag{4.23}$$

We adopt the notation $t:=p^{-1}$. For the left equality of (4.23), we observe that

$$1+t^2+t^3+\cdots=1+\frac{t^2}{1-t}=\frac{1-t+t^2}{1-t}=\frac{1+t^3}{(1+t)(1-t)}=\frac{1-t^6}{(1-t^2)\,(1-t^3)}\,. \tag{4.24}$$

Taking the product of this equation over all reciprocals t of primes and applying the Euler product formula (4.3) yields the desire equality.

For the right equality of (4.23), since

$$0<1-\frac{1+t^2+t^3+\cdots+t^n}{1+t^2+t^3+\cdots}=\frac{t^{n+1}+t^{n+2}+\cdots}{1+t^2+t^3+\cdots}<\frac{t^{n+1}+t^{n+2}+\cdots}{t^2+t^3+\cdots}=t^{n-1},$$

combining with (4.3), we obtain

$$1>\prod_t\frac{1+t^2+t^3+\cdots+t^n}{1+t^2+t^3+\cdots}>\prod_t\left(1-t^{n-1}\right)=\frac{1}{\zeta(n-1)}\to 1,\quad\text{as } n\to\infty$$

and complete the proof, where $\prod_t$ represents a product over all reciprocals t of primes.

One can also show the right equality of (4.23) using the fact that

$$1<1+p^{-2}+p^{-3}+\cdots+p^{-n}\uparrow 1+p^{-2}+p^{-3}+\cdots,\quad\text{as } n\to\infty \tag{4.25}$$

and the following version of monotone convergence theorem (which will also be very useful later in proving Theorem 4.13 (iii)).

Theorem 4.10. *If real numbers $x_{i,j}$ $(i,j=1,2,\dots)$ satisfy $1\leq x_{i,j}\uparrow x_i$ as $j\to\infty$ for all i, then we have*

$$\lim_{j\to\infty}\prod_{i=1}^{\infty}x_{i,j}=\prod_{i=1}^{\infty}x_i\,. \tag{4.26}$$

Here we allow the products and the limit to be infinity.

Proof. Applying the monotone convergence theorem to $\log x_{i,j}\,(\geq 0)$ gives

$$\lim_{j\to\infty}\sum_{i=1}^{\infty}\log x_{i,j}=\sum_{i=1}^{\infty}\log x_i\,.$$

Thus

$$\lim_{j\to\infty}\log\prod_{i=1}^{\infty}x_{i,j}=\log\prod_{i=1}^{\infty}x_i\,,$$

and (4.26) follows. □

Thanks to (4.25), we can apply Theorem 4.10 with $x_{i,j}=1+p_i^{-2}+p_i^{-3}+\cdots+p_i^{-j}$ and $x_i=1+p_i^{-2}+p_i^{-3}+\cdots$, and arrive at the desire equality. □

Remark 4.11. (1) The proof of Theorem 4.9 (iv) is reminiscent of (though not directly related to) [16, Exercise 1.186 (c)].

(2) Theorem 4.9 (i), (iv) and the numerical value of (iii) are obtained in [6, Section 3] via a slightly different approach. We have provided a complete and more detailed proof.

4.4.2. *More Generators (General ℓ).*

Now we consider the SNFs with at most $\ell\,(\leq n)$ diagonal entries not equal to 1, i.e., whose corresponding cokernel has at most ℓ generators. Denote the set of such $n\times n$ SNFs by $\mathcal{T}_n(\ell)$. In particular, when $\ell=n$, we have $\mu(\mathcal{T}_n(n))=1$. The above discussion on cyclic SNFs is for the case $\ell=1$. We will compute the density $\mu(\mathcal{T}_n(\ell))$ and its limit as $n\to\infty$, show that this limit increases to 1 as $\ell\to\infty$, and establish its asymptotics.

We start with a lemma which will play an important role in our proof (as well as in Section 5.2 below).

Lemma 4.12. *For any positive number $x\leq 1/2$, the positive sequence $\{[1/x,k]\}_{k=1}^{\infty}$ is decreasing and thus has a limit as $k\to\infty$:*

$$C(x):=(1-x)\,(1-x^2)\cdots\in\left[e^{-2x/(1-x)},1\right)\,. \tag{4.27}$$

This also implies that $C(x)\to 1$ as $x\to 0$ and that $[1/x,k]\in[e^{-2x/(1-x)},1)$ for all $x\in(0,1/2]$ and $k\geq 1$.

In particular, when $x=1/p$, we have

$$[p,k]\downarrow C_p:=C(1/p)\in\left[e^{-2/(p-1)},1\right)\subseteq\left[e^{-2},1\right)\,,\quad\text{as}\quad k\to\infty\,, \tag{4.28}$$

$C_p\to 1$ as $p\to\infty$, and $[p,k]\in[e^{-2/(p-1)},1)$ for all p and $k\geq 1$.

Proof. The sequence $[1/x,k]$ is strictly decreasing in k because $0<1-x^j<1$ for all $j\geq 1$.

To get the lower bound for $C(x)$, we will use the following inequality:

$$\ln y\geq-\frac{1-y}{y}\,,\quad\forall\ y\in(0,1]\,. \tag{4.29}$$

(To see this, let $\psi(y):=\ln y+(1-y)/y$, then $\psi'(y)=1/y-1/y^2\leq 0$. Hence $\psi(y)\leq\psi(1)=0$.)

Applying (4.29) with $y=1-x^j$ $(j\geq 1)$ yields

$$\ln\left(1-x^j\right)\geq-\frac{x^j}{1-x^j}\geq-2x^j \tag{4.30}$$

as $x^j\leq 1/2$. Summing up (4.30) over j from 1 to k, we get

$$\ln[1/x,k]\geq-\sum_{j=1}^{k}2x^j>-\sum_{j=1}^{\infty}2x^j=-\frac{2x}{1-x}\,.$$

Hence $C(x)=\lim_{k\to\infty}[1/x,k]\geq e^{-2x/(1-x)}$. □

Theorem 4.13. *We have*
(i)

$$\mu(\mathcal{T}_n(\ell)) = \prod_p Z_n(p,\ell) = \frac{1}{\prod_{i=2}^n \zeta(i)} \prod_p Y_n(p,\ell) =: Z_n(\ell)\,, \tag{4.31}$$

where

$$Z_n(p,\ell) = \mu_p(\mathcal{T}_n(\ell)) = [p,n] \sum_{i=0}^{\ell} \frac{p^{-i^2}[p,n]}{[p,i]^2[p,n-i]}\,,$$

$$Y_n(p,\ell) = \frac{[p,1]}{[p,n]} Z_n(p,\ell) = [p,1] \sum_{i=0}^{\ell} \frac{p^{-i^2}[p,n]}{[p,i]^2[p,n-i]}\,; \tag{4.32}$$

(ii)

$$Y_n(p,\ell) \uparrow [p,1] \sum_{i=0}^{\ell} \frac{p^{-i^2}}{[p,i]^2} =: Y(p,\ell) \quad \text{as} \quad n\to\infty\,, \quad Y(p,\ell) \uparrow \frac{[p,1]}{C_p} \quad \text{as} \quad \ell\to\infty\,, \tag{4.33}$$

and

$$\mu_p(\mathcal{T}_n(\ell)) = Z_n(p,\ell) \to \frac{C_p}{[p,1]} Y(p,\ell) = C_p \sum_{i=0}^{\ell} \frac{p^{-i^2}}{[p,i]^2} =: Z(p,\ell) \quad \text{as} \quad n\to\infty\,, \tag{4.34}$$

where $C_p = (1-p^{-1})(1-p^{-2})\cdots$ *as defined in* (4.28) *and* (4.27)*, then it follows from* (4.33) *that*

$$Z(p,\ell) \uparrow 1 \quad \text{as } \ell\to\infty\,; \tag{4.35}$$

(iii)

$$\mu(\mathcal{T}_n(\ell)) = Z_n(\ell) \to \frac{1}{\prod_{i=2}^{\infty} \zeta(i)} \prod_p Y(p,\ell) = \prod_p Z(p,\ell) =: Z(\ell) \quad \text{as} \quad n\to\infty\,, \tag{4.36}$$

and $Z(\ell) \uparrow 1$ *as* $\ell\to\infty$*;*
(iv)

$$\lim_{n\to\infty} \mu_p(\mathcal{T}_n(\ell)) = Z(p,\ell) = 1 - C_p^{-1} p^{-(\ell+1)^2} \left[1 - \frac{2}{p^2-p}\cdot p^{-\ell} + O\left(p^{-2\ell}\right)\right] \quad \text{as} \quad \ell\to\infty\,; \tag{4.37}$$

more precisely, this $O\left(p^{-2\ell}\right) \in (0, 2p^{-2\ell})$*;*
(v)

$$\lim_{n\to\infty} \mu(\mathcal{T}_n(\ell)) = Z(\ell) = 1 - C_2^{-1} \cdot 2^{-(\ell+1)^2} \left[1 - 2^{-\ell} + O\left(4^{-\ell}\right)\right] \quad \text{as} \quad \ell\to\infty\,, \tag{4.38}$$

where $C_2^{-1} \approx 3.46275$*.*

Parts (ii) *and* (iv) *also hold with* $p = 1/x$ *for any* $x \in (0, 1/2]$*.*

Figure 1 and Table 1 below illustrate the asymptotics (4.38) of $Z(\ell)$ and fast rate of convergence.

Remark 4.14. The convergence result (4.35) in Theorem 4.13 (ii) with $p = 1/x$ implies Euler's identity:

$$\sum_{i=0}^{\infty} \frac{x^{i^2}}{(1-x)^2(1-x^2)^2\cdots(1-x^i)^2} = \frac{1}{(1-x)(1-x^2)\cdots}\,.$$

FIGURE 1. Asymptotics of $Z(\ell)$

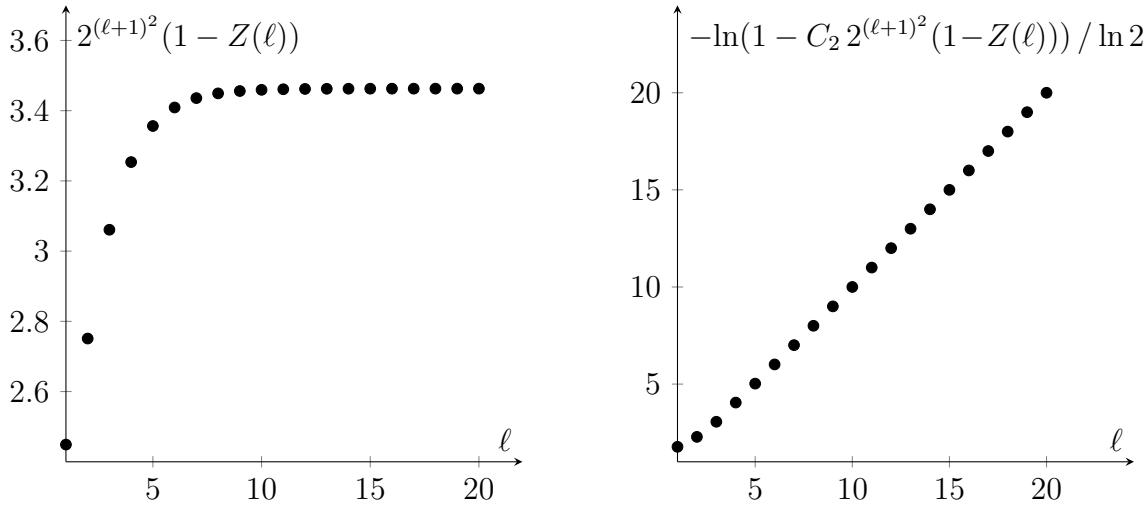

TABLE 1. Asymptotics of $Z(\ell)$

ℓ	$Z(\ell)$	$1-Z(\ell)$	$2^{(\ell+1)^2}(1-Z(\ell))$	$-\ln[1-C_2\,2^{(\ell+1)^2}(1-Z(\ell))]\,/\ln 2$
1	0.846935901735	$1.53064098265\times10^{-1}$	2.44902557224	1.77225611430
2	0.994626883543	$5.37311645734\times10^{-3}$	2.75103562616	2.28255339912
3	0.999953295075	$4.67049248389\times10^{-5}$	3.06085395424	3.10703467197
4	0.999999903035	$9.69645493161\times10^{-8}$	3.25359037644	4.04926385851
5	0.999999999951	$4.88413458245\times10^{-11}$	3.35635172814	5.02441603986
6	1.000000000000	$6.05577286766\times10^{-15}$	3.40909705378	6.01220652280
7	1.000000000000	$1.86255532064\times10^{-19}$	3.43580813230	7.00610418193
8	1.000000000000	$1.42657588960\times10^{-24}$	3.44924885316	8.00305233425
9	1.000000000000	$2.72629586798\times10^{-30}$	3.45599059345	9.00152622794
10	1.000000000000	$1.30126916909\times10^{-36}$	3.45936681921	10.0007631292

Proof. (i) The first equality follows from Theorem 3.8 with $\mathcal{S}=\mathcal{T}_n(\ell)$, $r=n-\ell$, $d_i=z=1$, $s_j=0$ for all i,j, and Theorem 3.2 with $s=1$, $a_1=n,n-1,\dots,n-\ell$, respectively.

The second equality follows from definition (4.32) and (4.21).

(ii) We observe that

$$\frac{[p,n]}{[p,n-i]}=\left(1-p^{-n}\right)\left(1-p^{-(n-1)}\right)\cdots\left(1-p^{-(n-i+1)}\right)\uparrow 1\ \text{ as }\ n\to\infty\,.$$

This leads to the first result of (4.33).

Since $Y_n(p,\ell)$ is also increasing in ℓ by definition (4.32), so is $Y(p,\ell)$, and for all $\ell\le n$, we have

$$Y_\ell(p,\ell)\le Y_n(p,\ell)\le Y_n(p,n)\,. \tag{4.39}$$

Further, we derive from

$$1=\mu_p(\mathcal{T}_n(n))=\frac{[p,n]}{[p,1]}Y_n(p,n)\,,$$

that

$$Y_n(p,n)=\frac{[p,1]}{[p,n]}\quad\text{and similarly,}\quad Y_\ell(p,\ell)=\frac{[p,1]}{[p,\ell]}\,.$$

Plugging into (4.39), we obtain

$$\frac{[p,1]}{[p,\ell]} \le Y_n(p,\ell) \le \frac{[p,1]}{[p,n]} < \frac{[p,1]}{C_p}\,.$$

Taking $n \to \infty$ yields

$$\frac{[p,1]}{[p,\ell]} \le Y(p,\ell) \le \frac{[p,1]}{C_p}\,.$$

Then taking $\ell \to \infty$ and applying Lemma 4.12 leads to the second result of (4.33).

Finally, on the strength of (4.33) and Lemma 4.12, we obtain (4.34) from definition (4.32):

$$Z_n(p,\ell) = \frac{[p,n]}{[p,1]} Y_n(p,\ell) \to \frac{C_p}{[p,1]} Y(p,\ell) \ \text{ as } \ n \to \infty\,.$$

This proof also carries over to $p = 1/x$ for any $x \in (0, 1/2]$.

(iii) It follows from definitions (4.31) and (4.32) that

$$Z_n(\ell) = \prod_p Z_n(p,\ell) = \prod_p \frac{[p,n]}{[p,1]} \prod_p Y_n(p,\ell)\,. \tag{4.40}$$

By virtue of (4.21), we have

$$\prod_p \frac{[p,n]}{[p,1]} = \frac{1}{\prod_{i=2}^n \zeta(i)} \to \frac{1}{\prod_{i=2}^\infty \zeta(i)} \approx 0.435757 \ \text{ as } \ n \to \infty\,. \tag{4.41}$$

Further, this limit

$$\frac{1}{\prod_{i=2}^\infty \zeta(i)} = \prod_{i=2}^\infty \prod_p \left(1 - p^{-i}\right) = \prod_p \prod_{i=2}^\infty \left(1 - p^{-i}\right) = \prod_p \frac{C_p}{[p,1]}\,.$$

Hence

$$\prod_p \frac{[p,n]}{[p,1]} \to \prod_p \frac{C_p}{[p,1]} \ \text{ as } \ n \to \infty\,. \tag{4.42}$$

We can also deduce (4.42) from Theorem 4.10 with $x_{i,j} = [p_i,1]/[p_i,j]$ since

$$1 \le \frac{[p,1]}{[p,n]} \uparrow \frac{[p,1]}{C_p} \ \text{ as } \ n \to \infty$$

by Lemma 4.12.

For the second product on the right-hand side of (4.40), from (4.20) in the proof of Theorem 4.9 (i), we see that $Y_n(p,1) = 1 + p^{-2} + p^{-3} + \cdots + p^{-n} > 1$. Since $Y_n(p,\ell)$ is increasing in ℓ, we have $Y_n(p,\ell) > 1$ as well. In conjunction with (4.33), we can apply Theorem 4.10 with $x_{i,j} = Y_j(p_i,\ell)$ to obtain

$$\prod_p Y_n(p,\ell) \uparrow \prod_p Y(p,\ell) \ \text{ as } \ n \to \infty\,. \tag{4.43}$$

Plugging (4.41), (4.43) and (4.42) into (4.40) along with definition (4.34) yields (4.36):

$$Z_n(\ell) \to \frac{1}{\prod_{i=2}^\infty \zeta(i)} \prod_p Y(p,\ell) = \prod_p \frac{C_p}{[p,1]} \prod_p Y(p,\ell) = \prod_p \frac{C_p}{[p,1]} Y(p,\ell) = \prod_p Z(p,\ell) \tag{4.44}$$

as $n \to \infty$.

Since $Y_n(p,\ell) > 1$ and $Y_n(p,\ell)$ is increasing in ℓ, so is $Y(p,\ell)$ (recall (4.33)). Thus we can apply Theorem 4.10 with $x_{i,j} = Y(p_i, j)$ to obtain

$$\prod_p Y(p,\ell) \uparrow \prod_p \frac{[p,1]}{C_p} \quad \text{as} \quad \ell \to \infty\,.$$

Finally, we plug this into the second expression of the limit of $Z_n(\ell)$ in (4.44):

$$Z(\ell) = \lim_{n\to\infty} Z_n(\ell) = \prod_p \frac{C_p}{[p,1]} \prod_p Y(p,\ell) \uparrow 1 \quad \text{as} \quad \ell \to \infty\,.$$

(iv) We prove for the more general case $p = 1/x$ with $x \in (0, 1/2]$. Let

$$V(x,\ell) := Z(1/x,\ell) = C(x) \sum_{i=0}^{\ell} \frac{x^{i^2}}{[1/x,i]^2}\,.$$

Recall that $C(x) = (1-x)(1-x^2)\cdots$ and $[1/x,i] = (1-x)(1-x^2)\cdots(1-x^i)$.

Since $V(x,\ell) = Z(1/x,\ell) \uparrow 1$ as $\ell \to \infty$ by (4.35), we have

$$\frac{1}{C(x)} = \sum_{i=0}^{\infty} \frac{x^{i^2}}{[1/x,i]^2} = \sum_{i=0}^{\ell} \frac{x^{i^2}}{[1/x,i]^2} + \sum_{i=\ell+1}^{\infty} \frac{x^{i^2}}{[1/x,i]^2} = \frac{V(x,\ell)}{C(x)} + \sum_{i=\ell+1}^{\infty} \frac{x^{i^2}}{[1/x,i]^2}\,.$$

Thus for any $x \in (0, 1/2]$, we obtain

$$x^{-(\ell+1)^2} C(x)\,[1 - V(x,\ell)] = x^{-(\ell+1)^2} C^2(x) \left[\frac{1}{C(x)} - \frac{V(x,\ell)}{C(x)}\right] = x^{-(\ell+1)^2} \sum_{i=\ell+1}^{\infty} \frac{C^2(x) x^{i^2}}{[1/x,i]^2}$$

$$= \sum_{i=\ell+1}^{\infty} x^{i^2-(\ell+1)^2} \prod_{j=i+1}^{\infty} \left(1-x^j\right)^2 = \prod_{j=\ell+2}^{\infty} \left(1-x^j\right)^2 + \sum_{i=\ell+2}^{\infty} x^{i^2-(\ell+1)^2} \prod_{j=i+1}^{\infty} \left(1-x^j\right)^2$$

$$= \left(1 - 2\sum_{j=\ell+2}^{\infty} x^j + \Delta_1\right) + \Delta_2 = 1 - \frac{2x^{\ell+2}}{1-x} + \Delta_1 + \Delta_2\,, \tag{4.45}$$

where

$$0 < \Delta_2 := \sum_{i=\ell+2}^{\infty} x^{i^2-(\ell+1)^2} \prod_{j=i+1}^{\infty} \left(1-x^j\right)^2 < \sum_{i=\ell+2}^{\infty} x^{i^2-(\ell+1)^2} < \sum_{i=2\ell+3}^{\infty} x^i = \frac{x^{2\ell+3}}{1-x} < x^{2\ell} \tag{4.46}$$

and

$$0 \le \Delta_1 := \prod_{j=\ell+2}^{\infty} \left(1-x^j\right)^2 - \left(1 - 2\sum_{j=\ell+2}^{\infty} x^j\right) \le 4 \sum_{j,j'\ge \ell+2} x^{j+j'} = \frac{4x^{2\ell+4}}{(1-x)^2} \le x^{2\ell}\,, \tag{4.47}$$

as $0 < x \le 1/2$, thanks to the inequality:

$$0 \le \prod_{i=1}^{u} (1-\delta_i) - \left(1 - \sum_{i=1}^{u} \delta_i\right) \le \sum_{1\le i<j\le u} \delta_i \delta_j$$

for $\delta_1, \delta_2, \ldots, \delta_u \in [0,1]$, which can be proved easily by induction on u (the left inequality was proved in (2.18). For the right inequality, base cases: $u = 1, 2$; inductive step from u to $u+1$: $(1-\delta_{u+1}) \prod_{i=1}^{u} (1-\delta_i) \le (1-\delta_{u+1})(1 - \sum_{i=1}^{u} \delta_i + \sum_{1\le i<j\le u} \delta_i\delta_j) = 1 - \sum_{i=1}^{u+1} \delta_i + \sum_{1\le i<j\le u+1} \delta_i\delta_j - \delta_{u+1} \sum_{1\le i<j\le u} \delta_i\delta_j \le 1 - \sum_{i=1}^{u+1} \delta_i + \sum_{1\le i<j\le u+1} \delta_i\delta_j$).

Plugging (4.46) and (4.47) into (4.45) yields (4.37).

(v) Since $Z(\ell)=\prod_p Z(p,\ell)$ by definition (4.36) and $0\le Z(p,\ell)\le 1$ for all p, we have $Z(\ell)\le Z(2,\ell)$. Thus it follows from (iv) that

$$Z(\ell)\le Z(2,\ell)=1-C_2^{-1}2^{-(\ell+1)^2}\left[1-2^{-\ell}+O\left(4^{-\ell}\right)\right] \quad \text{as} \quad \ell\to\infty\,. \tag{4.48}$$

On the other hand, we notice that when $\ell\ge 2$, the $O(p^{-2\ell})$ in (4.37) satisfies

$$O(p^{-2\ell})<2p^{-2\ell}\le\frac{2}{p^2}\cdot p^{-\ell}<\frac{2}{p^2-p}\cdot p^{-\ell}\,,$$

thus

$$Z(p,\ell)>1-C_p^{-1}p^{-(\ell+1)^2}\,.$$

Hence

$$Z(\ell)=\prod_p Z(p,\ell)>Z(2,\ell)\prod_{p\ge 3}\left(1-C_p^{-1}p^{-(\ell+1)^2}\right)\ge 1-(1-Z(2,\ell))-\sum_{p\ge 3}C_p^{-1}p^{-(\ell+1)^2}. \tag{4.49}$$

Here we took advantage of the inequality (2.18). Thanks to (4.28), the positive sum

$$\begin{aligned}\sum_{p\ge 3}C_p^{-1}p^{-(\ell+1)^2}&\le e^2\sum_{p\ge 3}p^{-(\ell+1)^2}=e^2\,2^{-(\ell+1)^2}\sum_{p\ge 3}\left(\frac{2}{p}\right)^{(\ell+1)^2}<\ e^2\,2^{-(\ell+1)^2}\sum_{p\ge 3}\left(\frac{2}{3}\right)^{\ell^2}\left(\frac{2}{p}\right)^2\\&<e^2\,2^{-(\ell+1)^2}\left(\frac{2}{3}\right)^{\ell^2}\cdot 4=2^{-(\ell+1)^2}O(4^{-\ell})\,.\end{aligned}$$

Finally, combining with (4.48) and (4.49) leads to (4.38). □

Remark 4.15. When $\ell=1$, in the proof of Theorem 4.9 we wrote $Y(1/x,1)$ as $(1-x^6)/(1-x^2)(1-x^3)$ (see (4.24)) in order to represent $Z(1)=\prod_p Y(p,1)\,/\prod_{i=2}^{\infty}\zeta(i)$ as the reciprocal of a product of values of the Riemann zeta function at positive integers. However, this is not the case when $\ell>1$; in fact, in general $Y(1/x,\ell)$ is not even a symmetric function in x, for instance,

$$Y\left(\frac{1}{x},2\right)=\frac{1-x-x^2+2x^3-x^5+x^6}{(1-x)^3(1+x)^2}\,,$$

$$Y\left(\frac{1}{x},3\right)=\frac{1-x-x^2+2x^4+x^5-2x^6-x^7+x^8+x^9-x^{11}+x^{12}}{(1-x)^5(1+x)^2(1+x+x^2)^2}\,.$$

5. Properties of the SNF Distribution Function μ_{p^s}

In this section, we first fix p,s,m,n and find the maximum and minimum of the probability density function μ_{p^s} of (3.1). Then we free p,s,m,n and study the monotonicity properties and limiting behaviors of $\mu_{p^s}(\{D_{\boldsymbol{a}}\})$, as a function of p,s,m,n and $\boldsymbol{a}$ (recall from Theorem 3.2 the notation of vector $\boldsymbol{a}=(a_1,a_2,\dots,a_s)$ as well as its corresponding diagonal matrix $D_{\boldsymbol{a}}\in\mathbb{S}$).

For convenience, we replace $m-a_i$ by b_i $(0\le i\le s)$ in (3.1) to get a simpler expression for $\mu_{p^s}(\{D_{\boldsymbol{a}}\})$:

$$f(p,s,m,n',\boldsymbol{b}):=p^{-\sum_{i=1}^{s}(n'+b_i)b_i}\cdot\frac{[p,n'+m][p,m]}{[p,n'+b_s][p,b_s]\prod_{i=1}^{s}[p,b_{i-1}-b_i]}\,. \tag{5.1}$$

Here and throughout this section, we shall assume that p is a prime, that s,m and n are positive integers, that $n>n':=n-m\ge 0$, and that $\boldsymbol{b}:=(b_1,b_2,\dots,b_s)$ is an integer vector satisfying $m=b_0\ge b_1\ge\cdots\ge b_s\ge 0$.

5.1. **The Maximum and Minimum.**

We show that $f(p,s,m,n',\cdot)$ attains its maximum at either $(0,0,\dots,0)$ or $(1,1,\dots,1)$ depending on p,s,m and n', and its minimum at $(m,m,\dots,m)$.

Theorem 5.1. *For fixed p,m,n and s, the maximum and minimum of $f(p,s,m,n',\cdot)$ are given as follows.*

(i) *If $p>2$, $s>1$ or $n'>0$, then*

$$\max_{b}\ f(p,s,m,n',\boldsymbol{b}) = \frac{[p,n'+m]}{[p,n']},$$

and the maximum is achieved if and only if $\boldsymbol{b}=(0,0,\dots,0):=\mathbf{0}$, in other words, if the corresponding matrix $D_{\boldsymbol{a}}$ is full rank;

(ii) *If $p=2$, $s=1$, $n'=0$ and $m>1$, then*

$$\max_{b}\ f(p,s,m,n',\boldsymbol{b}) = \frac{[2,m]^2}{[2,1][2,m-1]},$$

and the maximum is achieved if and only if $\boldsymbol{b}=(1)$;

(iii) *In both Case* (i) *and Case* (ii)*, we have*

$$\min_{b}\ f(p,s,m,n',\boldsymbol{b}) = p^{-s(n'+m)m},$$

and the minimum is achieved if and only if $\boldsymbol{b}=(m,m,\dots,m)$, in other words, if the corresponding matrix $D_{\boldsymbol{a}}$ is the zero matrix.

(iv) *If $p=2$, $s=1$, $n'=0$ and $m=1$, then $\boldsymbol{b}=(1)$ or (0), and they have the same value of f: $1/2$.*

Proof. (i) We proceed by the following two lemmas which show that the b_i's are all equal at the maximum of $f(p,s,m,n',\cdot)$, and that $b_i=0$ or 1 depending on p,s,m and n'.

Let $\boldsymbol{b}=(b_1,b_2,\dots,b_s)$ be an arbitrary s-tuple with $m=b_0\ge b_1\ge\cdots\ge b_s\ge 0$.

Lemma 5.2. *If $b_i>b_{i+1}$ for some $i\in\{1,2,\dots,s-1\}$ ($s\ge 2$), then we have*

$$f(p,s,m,n',\boldsymbol{b}')>f(p,s,m,n',\boldsymbol{b}),$$

where $\boldsymbol{b}'=(b_1',b_2',\dots,b_s')$ with $b_i'=b_i-1$ and $b_j'=b_j$ for all $j\ne i$. Note that $\boldsymbol{b}'$ still satisfies $m=b_0'\ge b_1'\ge\cdots\ge b_s'\ge 0$.

Lemma 5.3. *Let $\varphi(b):=f\big(p,s,m,n',(b,b,\dots,b)\big)$, $0\le b\le m$, then for all $0\le b<m$, we have*

$$\frac{\varphi(b)}{\varphi(b+1)}\begin{cases}<1, & \text{if } p=2,\ s=1,\ n'=0,\ m>1 \text{ and } b=0\\ =1, & \text{if } p=2,\ s=1,\ n'=0,\ m=1 \text{ and } b=0.\\ >1, & \text{otherwise}\end{cases}$$

These lemmas are proved right below this proof. Thanks to Lemma 5.2, the maximum point of $f(p,s,m,n',\cdot)$ must have the form $(b,b,\dots,b)$ with $0\le b\le m$. Therefore it reduces to finding the maximum of $\varphi(\cdot)$.

Since $p>2$, $s>1$ or $n'>0$, it follows from Lemma 5.3 that

$$\varphi(0)>\varphi(1)>\cdots>\varphi(m). \tag{5.2}$$

Hence the maximum of $\varphi(\cdot)$ is $\varphi(0)=\frac{[p,n'+m]}{[p,n']}$, as desired.

(ii) When $p=2$, $s=1$, $n'=0$ and $m>1$, it follows from Lemma 5.3 that

$$\varphi(0)<\varphi(1)\quad\text{and}\quad\varphi(1)>\cdots>\varphi(m). \tag{5.3}$$

Hence the maximum of $\varphi(\cdot)$ is $\varphi(1) = \frac{[2,m]^2}{[2,1][2,m-1]}$, as desired.

(iii) We proceed by the following lemma (proved right below this proof) which shows that at the minimum of $f(p,s,m,n',\cdot)$, all the b_i's ($i>1$) equal m.

Lemma 5.4. *If $b_i < b_{i-1}$ for some $i \in \{1,2,\ldots,s-1\}$ ($s \geq 2$), then we have*

$$f(p,s,m,n',\boldsymbol{b}') < f(p,s,m,n',\boldsymbol{b}),$$

where $\boldsymbol{b}' = (b_1', b_2', \ldots, b_s')$ with $b_i' = b_i + 1$ and $b_j' = b_j$ for all $j \neq i$. Note that $\boldsymbol{b}'$ still satisfies $m = b_0' \geq b_1' \geq \cdots \geq b_s' \geq 0$.

Thanks to Lemma 5.4, the minimum point of $f(p,s,m,n',\cdot)$ must have the form $(m,m,\ldots,m,b)$ with $0 \leq b \leq m$. Further, since $f\big(p,s,m,n',(m,m,\ldots,m,b)\big) = p^{-(s-1)(n'+m)m} \cdot \varphi(b)$ (by (5.1)), where φ is defined in Lemma 5.3 with $s=1$, it reduces to finding the minimum of $\varphi(\cdot)$.

Case (i) When $p>2$ or $n'>0$, it follows from (5.2) that the minimum of $\varphi(\cdot)$ is $\varphi(m) = p^{-(n'+m)m}$.

Case (ii) When $p=2$, $n'=0$ and $m>1$, it follows from (5.3) that the minimum of $\varphi(\cdot)$ is $\min\{\varphi(0),\varphi(m)\}$. Since

$$\varphi(0) = [2,m] > \left(1-2^{-1}\right)^m = 2^{-m} \geq 2^{-m^2} = \varphi(m),$$

the minimum of $\varphi(\cdot)$ is still $\varphi(m)$.

Hence the minimum of f is always $p^{-s(n'+m)m}$ and achieved at $(m,m,\ldots,m)$. □

Proof of Lemma 5.2. It follows from definition (5.1) that

$$\frac{f(p,s,m,n',\boldsymbol{b}')}{f(p,s,m,n',\boldsymbol{b})} = p^{(n'+b_i)b_i-(n'+b_i')b_i'} \cdot \frac{[p,b_{i-1}-b_i][p,b_i-b_{i+1}]}{[p,b_{i-1}-b_i'][p,b_i'-b_{i+1}]}$$
$$\geq p \cdot \frac{[p,b_{i-1}-b_i][p,b_i-b_{i+1}]}{[p,b_{i-1}-b_i+1][p,b_i-1-b_{i+1}]} = p \cdot \frac{1-p^{-(b_i-b_{i+1})}}{1-p^{-(b_{i-1}-b_i+1)}} > p\left(1-p^{-1}\right) = p-1 \geq 1,$$

as desired, where in the second last inequality, we used the condition that $b_i > b_{i+1}$ to get $1-p^{-(b_i-b_{i+1})} \geq 1-p^{-1}$. □

Proof of Lemma 5.3. By the definition of φ and (5.1), we obtain

$$\frac{\varphi(b)}{\varphi(b+1)} = p^{s[(n'+b+1)(b+1)-(n'+b)b]} \cdot \frac{[p,n'+b+1][p,b+1][p,m-b-1]}{[p,n'+b][p,b][p,m-b]}$$
$$= p^{s(n'+2b+1)} \cdot \frac{\left(1-p^{-(n'+b+1)}\right)\left(1-p^{-(b+1)}\right)}{1-p^{-(m-b)}} > p^{s(n'+2b+1)}\left(1-p^{-1}\right)^2, \tag{5.4}$$

where we used the fact that

$$1-p^{-(n'+b+1)},\ 1-p^{-(b+1)} \geq 1-p^{-1} \quad \text{and} \quad 1-p^{-(m-b)} < 1.$$

Case 1. $s(n'+2b+1) \geq 2$.

The right-hand side of (5.4) is at least

$$p^2\left(1-p^{-1}\right)^2 = (p-1)^2 \geq 1.$$

Case 2. $p \geq 3$.

The right-hand side of (5.4) is at least

$$p\left(1-p^{-1}\right)^2 \geq 3\left(1-3^{-1}\right)^2 = 4/3 > 1.$$

Case 3. $p=2$ and $s(n'+2b+1)=1$, which requires that $s=1$ and $n'=b=0$.

Plugging into (5.4) yields

$$\frac{\varphi(b)}{\varphi(b+1)} = \frac{2\left(1-2^{-1}\right)^2}{1-2^{-m}} = \frac{1}{2-2^{1-m}} \begin{cases} <1, & \text{if } m>1 \\ =1, & \text{if } m=1 \end{cases}$$

and completes the proof. □

Proof of Lemma 5.4. By definition (5.1), we obtain

$$\frac{f(p,s,m,n',\boldsymbol{b}')}{f(p,s,m,n',\boldsymbol{b})} = p^{(n'+b_i)b_i-(n'+b_i')b_i'} \cdot \frac{[p,b_{i-1}-b_i][p,b_i-b_{i+1}]}{[p,b_{i-1}-b_i'][p,b_i'-b_{i+1}]}$$

$$\le p^{-1} \cdot \frac{[p,b_{i-1}-b_i][p,b_i-b_{i+1}]}{[p,b_{i-1}-b_i-1][p,b_i+1-b_{i+1}]} = \; p^{-1} \cdot \frac{1-p^{-(b_{i-1}-b_i)}}{1-p^{-(b_i+1-b_{i+1})}} < p^{-1} \cdot \frac{1}{1-p^{-1}} = \frac{1}{p-1} \le 1\,,$$

as desired, where in the second last inequality, we used the condition that $b_i \ge b_{i+1}$ to get $1 - p^{-(b_i+1-b_{i+1})} \ge 1-p^{-1}$. □

5.2. **Monotonicity Properties and Limiting Behaviors.**

Now we free p, s, m and n'. We will see that the monotonicity properties and limiting behaviors of f of (5.1) when $\boldsymbol{b} = \boldsymbol{0}$ (i.e., the corresponding matrix $D_{\boldsymbol{a}}$ is full rank) differ tremendously from those when $\boldsymbol{b} \ne \boldsymbol{0}$. Specifically, we show that f is increasing in n', p and decreasing in m when $\boldsymbol{b} = \boldsymbol{0}$ (Theorem 5.5), but decreasing in n' and increasing in m when $\boldsymbol{b} \ne \boldsymbol{0}$ (Theorem 5.6). Further, with regard to limiting behaviors, when $\boldsymbol{b} = \boldsymbol{0}$, the limit of f as p, m or $n' \to \infty$ is positive (note that f is independent of s) (Theorem 5.5); whereas when $\boldsymbol{b} \ne \boldsymbol{0}$, the limit of f is still positive as $m \to \infty$ or $s \to \infty$ with $\sum_{i=1}^{s} b_i$ bounded (Theorems 5.10, 5.11), but zero as $\max\{p, n', \sum_{i=1}^{s} b_i\} \to \infty$ (Theorems 5.7, 5.9). Lemma 4.12 is crucial in the analysis of limiting behaviors of f.

5.2.1. *The Case of* $\boldsymbol{b} = \boldsymbol{0}$.

Let

$$f_0(p,m,n') := f(p,s,m,n',\boldsymbol{0}) = \frac{[p,n'+m]}{[p,n']} = \prod_{j=n'+1}^{n'+m} \left(1-p^{-j}\right). \tag{5.5}$$

We derive the following monotonicity properties and limiting behaviors of f_0 with the help of Lemma 4.12.

Theorem 5.5. *The function $f_0(p,m,n')$ of (5.5) is strictly increasing in p, n' while strictly decreasing in m, and satisfies*

$$\lim_{m\to\infty} f_0(p,m,n') = \frac{C_p}{[p,n']} < 1\,, \quad \lim_{n'\to\infty} \inf_m f_0(p,m,n') = 1 \quad \text{and} \quad \lim_{p\to\infty} \inf_{m,n'} f_0(p,m,n') = 1\,,$$

where $C_p = (1-p^{-1})(1-p^{-2})\cdots$ as defined in Lemma 4.12. In particular, we have

$$\lim_{m\to\infty} f_0(p,m,0) = C_p \quad \text{and} \quad \lim_{n'\to\infty} f_0(p,m,n') = 1 = \lim_{p\to\infty} f_0(p,m,n')\,;$$

the first equality characterizes C_p as the limit of the probability that a random $m \times m$ integer matrix over $\mathbb{Z}/p^s\mathbb{Z}$ is nonsingular as $m \to \infty$.

Proof. Utilizing the expression on the right-hand side of (5.5), we obtain the monotonicities. Then we apply Lemma 4.12 to get

$$\inf_m f_0(p,m,n') = \lim_{m\to\infty} f_0(p,m,n') = \frac{C_p}{[p,n']} \to \frac{C_p}{C_p} = 1 \quad \text{as} \;\; n' \to \infty\,,$$

and

$$\inf_{m,n'} f_0(p,m,n') = \lim_{m\to\infty} f_0(p,m,0) = C_p \to 1 \quad \text{as} \quad p\to\infty\,.$$

□

5.2.2. *The Case of* $\boldsymbol{b}\neq\mathbf{0}$.

We first present the monotonicity properties of $f(p,s,m,n',\boldsymbol{b})$ in n' and m.

Theorem 5.6. *Suppose that* $\boldsymbol{b}\neq\mathbf{0}$. *The function* $f(p,s,m,n',\boldsymbol{b})$ *is strictly decreasing in* n' *while strictly increasing in* m.

Proof. Recall that $b_1\geq b_2\geq\cdots b_s\geq 0$. Since $\boldsymbol{b}\neq\mathbf{0}$, we have $b_1\geq 1$. Thus the ratio

$$\frac{f(p,s,m,n'+1,\boldsymbol{b})}{f(p,s,m,n',\boldsymbol{b})} = p^{-\sum_{i=1}^s (n'+1+b_i)b_i+\sum_{i=1}^s (n'+b_i)b_i}\cdot\frac{[p,n'+1+m][p,n'+b_s]}{[p,n'+m][p,n'+1+b_s]}$$
$$= p^{-\sum_{i=1}^s b_i}\cdot\frac{1-p^{-(n'+1+m)}}{1-p^{-(n'+1+b_s)}} < p^{-1}\cdot\frac{1}{1-p^{-1}} = \frac{1}{p-1}\leq 1\,,$$

and

$$\frac{f(p,s,m+1,n',\boldsymbol{b})}{f(p,s,m,n',\boldsymbol{b})} = \frac{[p,n'+m+1][p,m+1][p,m-b_1]}{[p,n'+m][p,m][p,m+1-b_1]}$$
$$= \frac{\left(1-p^{-(n'+1+m)}\right)\left(1-p^{-(m+1)}\right)}{1-p^{-(m+1-b_1)}} \geq \frac{\left(1-p^{-(m+1)}\right)^2}{1-p^{-m}} > \frac{1-2p^{-(m+1)}}{1-p^{-m}}\geq 1\,,$$

as $p\geq 2$. □

Recall from definition (5.1) that f is the product of a power of p

$$f_1(p,s,m,n',\boldsymbol{b}) := p^{-\sum_{i=1}^s (n'+b_i)b_i}$$

and a fraction

$$f_2(p,s,m,n',\boldsymbol{b}) := \frac{[p,n'+m][p,m]}{[p,n'+b_s][p,b_s]\prod_{i=1}^s [p,b_{i-1}-b_i]}\,. \tag{5.6}$$

When s is fixed, thanks to Lemma 4.12, the function f_2 defined in (5.6) is bounded regardless of the values of other variables. Moreover, when m (instead of s) is fixed, this result also holds since $\sum_{i=1}^s (b_{i-1}-b_i) = m-b_s\leq m$ implies that

$$\prod_{i=1}^s [p,b_{i-1}-b_i] = \prod_{i=1}^s\prod_{j=1}^{b_{i-1}-b_i}\left(1-p^{-j}\right)\geq\left(1-p^{-1}\right)^m\geq 2^{-m}\,.$$

These observations lead to the following zero limiting probabilities.

Theorem 5.7. *We have*

$$\lim_{\max\left\{p,n',\sum_{i=1}^s b_i\right\}\to\infty,\,\boldsymbol{b}\neq\mathbf{0}} \max_m f(p,s,m,n',\boldsymbol{b}) = 0 \quad \textit{when } s \textit{ is fixed}$$

and

$$\lim_{\max\left\{p,n',\sum_{i=1}^s b_i\right\}\to\infty,\,\boldsymbol{b}\neq\mathbf{0}} f(p,s,m,n',\boldsymbol{b}) = 0 \quad \textit{when } m \textit{ is fixed.}$$

Proof. When s or m is fixed, we have shown that f_2 is bounded. On the other hand, we have

$$f_1(p,s,m,n',\boldsymbol{b}) = p^{-\sum_{i=1}^s (n'+b_i)b_i} = p^{-n'\sum_{i=1}^s b_i-\sum_{i=1}^s b_i^2}\to 0$$

as long as $\boldsymbol{b} \neq \mathbf{0}$ and

$$\max\left\{p, n'\sum_{i=1}^{s} b_i + \sum_{i=1}^{s} b_i^2\right\} \to \infty\,. \tag{5.7}$$

Noticing that

$$n'\sum_{i=1}^{s} b_i \le n'\sum_{i=1}^{s} b_i + \sum_{i=1}^{s} b_i^2 \le n'\sum_{i=1}^{s} b_i + \left(\sum_{i=1}^{s} b_i\right)^2\,,$$

thus (5.7) is equivalent to $\max\{p, n', \sum_{i=1}^{s} b_i\} \to \infty$. □

Remark 5.8. Let $r\,(\le s)$ be the number of nonzeroes in $\{b_1, b_2, \ldots, b_s\}$, i.e., $b_r > 0 = b_{r+1}$ (we define $b_{s+1} = 0$), then $rb_r\,, b_1 \le \sum_{i=1}^{s} b_i \le rb_1$ due to the decreasing property of the b_i's. Hence $\sum_{i=1}^{s} b_i \to \infty$ if and only if $\max\{b_1, r\} \to \infty$. In particular, when s is fixed, we have $\sum_{i=1}^{s} b_i \to \infty$ if and only if $b_1 \to \infty$.

Moreover, if we free s, m, n' but fix p and let $\sum_{i=1}^{s} b_i \to \infty$, then f also goes to 0.

Theorem 5.9. *For a fixed prime p, we have*

$$\lim_{\sum_{i=1}^{s} b_i \to \infty} \max_{m,n'} f(p, s, m, n', \boldsymbol{b}) = 0\,.$$

Proof. Since $\sum_{i=1}^{s} b_i \to \infty$, we can assume that $\boldsymbol{b} \neq \mathbf{0}$. Moreover, if $r\,(\le s)$ is the number of nonzeroes in $\{b_1, b_2, \ldots, b_s\}$, then $\max\{b_1, r\} \to \infty$ (see Remark 5.8), which is equivalent to that $b_1 \to \infty$ or $r \to \infty$ holds.

Case 1. $b_1 \to \infty$.

For any fixed p, s, m and n, from Lemma 5.2 we see that for $\boldsymbol{b}' = (b_1, b_s, b_s, \ldots, b_s)$,

$$\begin{aligned} &f(p, s, m, n', \boldsymbol{b}) \le f(p, s, m, n', \boldsymbol{b}') \\ &= p^{-(n'+b_1)b_1-(s-1)(n'+b_s)b_s} \cdot \frac{[p, n'+m][p, m]}{[p, n'+b_s][p, b_s][p, m-b_1][p, b_1-b_s]} \le p^{-b_1} \cdot \frac{1}{(e^{-2})^4} \end{aligned}$$

on the strength of Lemma 4.12. Hence

$$\max_{m,n'} f(p, s, m, n', \boldsymbol{b}) \le p^{-b_1} \cdot \frac{1}{(e^{-2})^4} \to 0\,, \quad \text{as} \;\; b_1 \to \infty\,.$$

Case 2. $r \to \infty$.

For any fixed p, s, m and n, from Lemma 5.2 we see that for $\boldsymbol{b}' = (b_r, b_r, \ldots, b_r, b_s, b_s, \ldots, b_s)$ (with r b_r's and $(s-r)$ b_s's),

$$\begin{aligned} &f(p, s, m, n', \boldsymbol{b}) \le f(p, s, m, n', \boldsymbol{b}') \\ &= p^{-r(n'+b_r)b_r-(s-r)(n'+b_s)b_s} \cdot \frac{[p, n'+m][p, m]}{[p, n'+b_s][p, b_s][p, m-b_r][p, b_r-b_s]} \le p^{-r} \cdot \frac{1}{(e^{-2})^4}\,, \end{aligned}$$

on the strength of Lemma 4.12. Hence

$$\max_{m,n'} f(p, s, m, n', \boldsymbol{b}) \le p^{-r} \cdot \frac{1}{(e^{-2})^4} \to 0\,, \quad \text{as} \;\; r \to \infty\,.$$

□

All the limits of f we have found so far equal zero. To attain a nonzero limit, we must have a bounded $\max\{p, n', \sum_{i=1}^{s} b_i\}$. We may fix $p, s, n', \boldsymbol{b}$, let $m \to \infty$ and apply Lemma 4.12.

Theorem 5.10. *For fixed p, s, n' and $\boldsymbol{b} \neq \mathbf{0}$, we have*

$$\lim_{m\to\infty} f(p, s, m, n', \boldsymbol{b}) = p^{-\sum_{i=1}^{s}(n'+b_i)b_i} \cdot \frac{C_p}{[p, n'+b_s][p, b_s]\prod_{i=2}^{s}[p, b_{i-1}-b_i]}\,.$$

We may also weaken the constraints by fixing p, n' and $\sum_{i=1}^{s} b_i$ only. A natural way to achieve this is to fix the first few b_i's, say $b_1, b_2, \ldots, b_r$ ($r < s$ fixed), and set the rest to be zero no matter how big s is. According the definition (5.1) of f, for $\boldsymbol{b} = (b_1, b_2, \ldots, b_r, 0, 0, \ldots, 0)$, we have

$$f(p, s, m, n', \boldsymbol{b}) = p^{-\sum_{i=1}^{r}(n'+b_i)b_i} \cdot \frac{[p, n'+m][p, m]}{[p, n'] \prod_{i=1}^{r+1} [p, b_{i-1} - b_i]}, \tag{5.8}$$

which is independent of s. Coupling with Theorem 5.9 gives the following.

Theorem 5.11. *When m, n' and p are fixed, for any given infinite integer sequence $\{b_0, b_1, \ldots\}$ with $m = b_0 \geq b_1 \geq \cdots \geq b_i \geq b_{i+1} \geq \cdots \geq 0$, we have*

$$\lim_{s\to\infty} f(p, s, m, n', \boldsymbol{b}^s) = \begin{cases} 0, & \text{if } \sum_{i=1}^{\infty} b_i \to \infty \\ p^{-\sum_{i=1}^{r}(n'+b_i)b_i} \cdot \frac{[p,n'+m][p,m]}{[p,n'] \prod_{i=1}^{r+1} [p, b_{i-1}-b_i]}, & \text{otherwise} \end{cases},$$

where $\boldsymbol{b}^s := (b_0, b_1, \ldots, b_s)$ and in the second case, r is the number of nonzeroes in $\{b_0, b_1, \ldots\}$ and finite (see Remark 5.8), and $b_{r+1} = 0$.

References

[1] Akemann, G., Baik, J. & Di Francesco, P. (2011) *The Oxford Handbook of Random Matrix Theory*. Oxford University Press, Oxford. MR2920518

[2] Anderson, G.W., Guionnet, A. & Zeitouni, O. (2010) *An Introduction to Random Matrices*. Cambridge University Press, Cambridge. MR2760897

[3] Bôcher, M. (1964) *Introduction to Higher Algebra*. Dover Publications, Inc., New York. MR0172882

[4] Cohen, H. & Lenstra, H.W., Jr. (1984) Heuristics on class groups. *Number theory (New York 1982)*, Lecture Notes in Math. **1052**, 26–36, Springer, Berlin. MR0750661

[5] Cohen, H. & Lenstra, H.W., Jr. (1984) Heuristics on class groups of number fields. *Number theory (Noordwijkerhout 1983)*, Lecture Notes in Math. **1068**, 33–62, Springer, Berlin. MR0756082

[6] Ekedahl, T. (1991) An infinite version of the Chinese remainder theorem. *Comment. Math. Univ. St. Paul.* **40**(1), 53–59. MR1104780

[7] Feng, C., Nóbrega, R.W., Kschischang, F.R., & Silva, D. (2013) Communication over finite-ring matrix channels. *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 2890–2894.

[8] Feng, C., Nóbrega, R.W., Kschischang, F.R., & Silva, D. (2014) Communication over finite-chain-ring matrix channels. *IEEE Trans. Inform. Theory* **60**(10), 5899–5917. MR3265002

[9] Friedman, E. & Washington L.C. (1989) On the distribution of divisor class groups of curves over a finite field. *Théorie des nombres (Quebec, PQ, 1987)*, 227–239, de Gruyter, Berlin. MR1024565

[10] Fulman, J. (2002) Random matrix theory over finite fields. *Bull. Amer. Math. Soc. (N.S.)* **39**(1), 51–85. MR1864086

[11] Lang, S. & Weil, A. (1954) Number of points of varieties in finite fields. *Amer. J. Math.* **76**, 819–827. MR0065218

[12] Mehta, M.L. (2004) *Random Matrices*. Third ed. Elsevier/Academic Press, Amsterdam. MR2129906

[13] Nguyen, P.Q. & Shparlinski, I.E. (2015) Counting co-cyclic lattices. *Preprint*, available at http://arxiv.org/abs/1505.06429.

[14] Poonen, B. (2003) Squarefree values of multivariable polynomials. *Duke Math. J.* **118**(2), 353–373. MR1980998

[15] Poonen, B. & Stoll, M. (1999) The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)* **150**(3), 1109–1149. MR1740984

[16] Stanley, R.P. (2011) *Enumerative Combinatorics*. Vol. 1, second ed., Cambridge University Press, Cambridge. MR2868112

[17] Wood, M.M. (2015) Random integral matrices and the Cohen Lenstra Heuristics. *Preprint*, available at http://arxiv.org/abs/1504.04391.

E-mail address: yinghui@math.columbia.edu, yinghui@alum.mit.edu

Department of Mathematics, Columbia University, New York, New York 10027

E-mail address: rstan@math.mit.edu

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139